Whitepaper

Het model-DSP als risicoclassificatie

Voor informatiebeveiliging, privacy en duurzame toegankelijkheid

vhic bron van vernieuwing

Colofon

Uitgever:	VHIC, Einsteinlaan 26a, 2289 CC Rijswijk, www.vhic.nl
Auteurs:	Marije de Mooij
Versie:	3.0
Publicatiedatum:	31 maart 2022

Deze whitepaper heeft betrekking op VIND Informatiemanagement.
VIND Informatiemanagement is een gezamenlijk product van Sdu en VHIC.

Voor vragen over VIND Informatiemanagement kunt u terecht bij Sdu:
https://www.sdu.nl/vind-informatiebeheer

Inhoud

1. Rubricering of classificatie van informatie

Niet alle informatie waarover uw organisatie beschikt is even belangrijk. Informatiemanagement zou zich met name moeten richten op *die* informatie die, wanneer niet goed beheerd, tot grote negatieve consequenties kan leiden. Een effectieve inzet van de beschikbare informatiemanagementmiddelen vergt inzicht in het belang van informatie.

Om dit inzicht te verkrijgen is kennis nodig van de rol van informatie in uw processen en van het belang van deze processen. Wanneer het ontbreken van de juiste informatie ertoe leidt dat processen niet goed worden uitgevoerd zijn de consequenties hiervan immers een belangrijke indicator voor de 'waarde' van de informatie.

Een nuttig instrument om het belang van informatie te bepalen is de risicoanalyse: welke risico's lopen de organisatie en/of andere belanghebbenden wanneer de betreffende informatie niet goed wordt beheerd en er als gevolg daarvan geen garantie kan worden gegeven dat de vertrouwelijkheid, integriteit en beschikbaarheid ervan zijn gewaarborgd. De uitkomst van de risicoanalyse is een classificatie of rubricering van de informatie in risico-categorieën (meestal laag, midden en hoog).

In de model-DSP's voor gemeenten, waterschappen, corporaties en het onderwijs zijn voor alle processen en registraties die deel uitmaken van deze modellen deze risicoanalyses reeds uitgevoerd. De resultaten hiervan zijn terug te vinden in de i-Navigator (versie 3.2 en hoger). In deze whitepaper wordt toegelicht hoe de redactie dit heeft aangepakt en er wordt een verantwoording gegeven voor de hierbij gemaakte keuzes. De risicoanalyses zijn uitgevoerd vanuit een drietal invalshoeken:

- Informatieveiligheid, uitgesplitst naar vertrouwelijkheid (vanuit een organisatieperspectief), integriteit en beschikbaarheid (vanuit een bedrijfsvoeringsperspectief);
- privacybescherming (vertrouwelijkheid vanuit een betrokkene-perspectief);
- duurzame toegankelijkheid (beschikbaarheid vanuit een verantwoordings- en een erfgoedperspectief).

Informatieveiligheid en de BIO

Informatieveiligheid is een belangrijk aspect van informatiemanagement binnen gemeenten en andere (semi-)overheidsinstellingen. Om organisaties te helpen grip te krijgen op deze materie is vanuit een overheidsbreed initiatief de Baseline Informatiebeveiliging Overheid (BIO) ontwikkeld. De BIO bevat ongeveer 250 eisen waaraan een overheidsinstelling zou moeten voldoen om met recht te mogen claimen dat de informatieveiligheid op orde is. De BIO schrijft voor dat organisaties Business Impact Analyses (BIA's) uitvoeren om per proces en/of per informatiesysteem vast te stellen welke risico's de organisatie loopt wanneer vertrouwelijkheid, integriteit en beschikbaarheid van informatie niet op orde zijn.

Privacybescherming en de AVG

Voor alle organisaties geldt de Algemene Verordening Gegevensbescherming (AVG) waarin de bescherming van persoonsgegevens wettelijk is geregeld. Deze schrijft voor dat organisaties Privacy Impact Analyses (PIA's) moeten uitvoeren om vast te stellen welke risico's *betrokkenen* lopen wanneer de vertrouwelijkheid van hun persoonsgegevens niet voldoende is gewaarborgd.

Duurzame toegankelijkheid en de Archiefwet

De archiefwet regelt dat overheidsinstellingen de informatieobjecten waarvoor zij verantwoordelijk zijn in goede, geordende en toegankelijke staat brengen en bewaren totdat zij in aanmerking komen voor overbrenging of vernietiging. De handreiking kwaliteitssysteem Informatiebeheer Decentrale Overheden (KIDO) schrijft daarom voor dat overheidsorganisaties de onder hen berustende archiefbescheiden classificeren op basis van risicocategorieën en daarvoor toepasselijke beheerregimes vaststellen.

1.1 Gehanteerde terminologie

We sluiten in deze whitepaper waar mogelijk aan bij de terminologie die gehanteerd wordt in wet- en regelgeving en in de relevante normenkaders (AVG, Archiefwet, BIO, KIDO, ...). Om onduidelijkheden te voorkomen vatten we hier de belangrijkste begrippen kort samen.

Business Impact analyse (BIA)

Een BIA is een per proces of per informatiesysteem uitgevoerde analyse met betrekking tot de risico's die de organisatie loopt wanneer de beschikbaarheid, de integriteit en de vertrouwelijkheid (BIV) van de informatie in het proces of het systeem niet is gewaarborgd. De Informatie Beveiligingsdienst (IBD) hanteert voor deze begrippen de volgende definities:

- **Beschikbaarheid**: hoeveel en wanneer data toegankelijk is en gebruikt kan worden.
- **Integriteit**: het in overeenstemming zijn van informatie met de werkelijkheid en dat niets ten onrechte is achtergehouden of verdwenen (juistheid, volledigheid en tijdigheid).
- **Vertrouwelijkheid**: de bevoegdheden en de mogelijkheden tot muteren, kopiëren, toevoegen, vernietigen of kennisnemen van informatie voor een gedefinieerde groep van gerechtigden.

Een BIA leidt dus per proces of informatiesysteem tot drie classificaties (gezamenlijk de BIV-classificaties genoemd).

Privacy Impact Analyse (PIA)

Een PIA[1] is vergelijkbaar met een BIA maar hier gaat het om een analyse van de risico's die de organisatie *en de betrokkene* lopen wanneer persoonsgegevens in een proces of informatiesysteem niet voldoende worden beschermd.

Basisbeveiligingsniveau (BBN)

Een basisbeveiligingsniveau is een vaststelling van het vereiste beveiligingsniveau van een proces of informatiesysteem op basis van de uitkomst van de uitgevoerde BIA's en PIA's. De mogelijke niveaus zijn BBN1 (laag), BBN2 (midden), BBN2+ (hoog) en BBN3 (zeer hoog). De BBN-classificatie wordt in de BIO gebruikt om te bepalen welke eisen en maatregelen uit de norm van toepassing zijn op welke processen en welke systemen. Wanneer voor een proces of informatiesysteem de BIV-classificaties bekend zijn kan het basisbeveiligingsniveau hieruit worden afgeleid op basis van de regels die zijn beschreven in de BIO (bijlage 2 van de BIO).

Risicoclassificatie (of informatieclassificatie)

Een risicoclassificatie[2] is een overzicht van alle informatie in de organisatie geclassificeerd naar gewenste beschikbaarheid, integriteit en vertrouwelijkheid. Het doel van deze classificatie is om te zorgen voor een passend beschermingsniveau voor alle informatie binnen een organisatie. Om tot een volwaardige risicoclassificatie te komen is het noodzakelijk om voor alle processen en informatiesystemen een BIA uit te voeren. Vanwege de hoeveelheid werk die dit met zich meebrengt (zie volgende paragraaf) staat het ontwikkelen van een dergelijk overzicht bij veel organisaties nog in de kinderschoenen.

2. Issues met de standaardaanpak

De 'standaardvorm' waarin een risicoanalyse wordt uitgevoerd is dat er in een workshopachtige setting met betrokken teamleden aan de hand van een checklist wordt gekeken wat de impact zou kunnen zijn van

[1] Internationaal wordt dit DPIA genoemd: Data Protection Impact Analysis

[2] Het begrip 'risicoclassificatie' is afkomstig uit het Voorschrift Informatiebeveiliging Rijksdienst 1994. De BIO gebruikt hiervoor de term 'informatieclassificatie'. De strekking van beide begrippen is identiek.

incidenten. Bij PIA's gaat het dan om incidenten met betrekking tot privacy, bij BIA's om incidenten met betrekking tot beschikbaarheid, integriteit en vertrouwelijkheid en bij een risicoanalyse voor de archiefwet om incidenten met betrekking tot de toegankelijkheid van informatie. Om tot een complete risicoclassificatie te komen is het nodig om voor *alle* processen en systemen deze analyses uit te voeren. Dit geldt in ieder geval voor de processen en systemen waarvan niet op voorhand kan worden vastgesteld dat er geen enkel informatieveiligheids- of privacyrisico is. Een simpele rekensom toont aan dat dit een enorme hoeveelheid werk met zich meebrengt. Volgens het model-DSP voor Gemeenten heeft een Nederlandse gemeente ongeveer duizend processen. In 70% van deze processen worden persoonsgegevens verwerkt waardoor ze alleen al om die reden in aanmerking komen voor een BIA en PIA.

Omdat het ondoenlijk is 700 à 1000 workshops te organiseren wordt er vaak voor gekozen om alleen risicoanalyses uit te voeren voor de meest kritische processen en systemen. Maar dit veronderstelt dat de organisatie op voorhand al weet wat de kritische processen zijn met betrekking tot informatieveiligheid en privacy! En bovendien, voor die processen en systemen waarvan je op je vingers kunt natellen dat incidenten een grote impact zullen hebben zijn waarschijnlijk de benodigde maatregelen ook al wel getroffen. Incidenten vinden juist meestal plaats waar je ze niet verwacht. Het gezegde luidt niet voor niets dat een ongeluk in een klein hoekje zit...

Een tweede issue met de 'standaardaanpak' is de workshopvorm. Terecht wordt ervan uitgegaan dat de betrokkenen bij het proces of systeem kennis hebben van de mogelijke *consequenties* van incidenten. Het is echter maar zeer de vraag of deze 'leken' op het gebied van risicomanagement ook tot goede *risico-inschattingen* kunnen komen. Bovendien blijken de in de BIO gehanteerde risico categorieën, ondanks de nadere uitleg die gegeven wordt, in de praktijk moeilijk te operationaliseren. Het vraagt enige ervaring om deze categorieën consistent te hanteren. Omdat juist deze ervaring ontbreekt bij de proces- en systeembetrokkenen is er een groot risico dat er grote inconsistenties ontstaan in de uitkomsten van de BIA's en PIA's.

Kortom, de hier geschetste standaardaanpak maakt het onmogelijk om tot een complete en consistente risicoclassificatie te komen.

3. Het model-DSP

Een documentair structuurplan (DSP) beschrijft de informatiehuishouding van een organisatie. Een compleet DSP bevat een inventarisatie van alle processen, alle registraties en alle informatiesystemen binnen een organisatie inclusief hun onderlinge verbanden. Per proces en registratie is middels metadata vastgelegd welke informatie een rol speelt, wat de kenmerken zijn van die informatie en hoe die informatie moet worden beheerd. De kerngedachte achter het DSP is dat het binnen de organisatie geldt als Single Point of Truth (SPOT) met betrekking tot processen en informatie. Het model-DSP fungeert als procesinventarisatie, als zaaktypecatalogus voor het zaaksysteem, als verwerkingsregister voor de AVG en – nu ook – als risicoclassificatie voor de BIO en de Archiefwet.

Gelijksoortige organisaties zullen over het algemeen een gelijksoortige informatiehuishouding hebben. Met dit in het achterhoofd hebben Sdu en VHIC een aantal model-DSP's op de markt gebracht (o.a. voor gemeenten, waterschappen, provincies, veiligheidsregio's en onderwijsinstellingen). Deze model-DSP's worden onderhouden door een centrale redactie en worden geleverd met tooling (de i-Navigator) waarmee het model aangepast kan worden naar de eigen organisatie.

3.1 Het model-DSP als risicoclassificatie

Processen en registraties

Uit de voorgaande paragrafen blijkt dat het zelf ontwikkelen van een complete risicoclassificatie op basis van BIA's en PIA's een onevenredige inspanning vraagt en bovendien tot een twijfelachtig resultaat kan leiden. Met dit in het achterhoofd heeft de model-DSP redactie ervoor gekozen om een 'model-risicoclassificatie' toe te voegen aan het model-DSP. Hiervoor is per proces en per registratie een BIA/PIA uitgevoerd en zijn de resultaten hiervan

vastgelegd op het tabblad BIO in de i-Navigator (3.2 en hoger). Voor elk proces en elke registratie zijn de volgende classificaties toegevoegd:

- Classificatie beschikbaarheid (waarden Laag, Midden, Hoog)
- Classificatie integriteit (waarden Laag, Midden, Hoog)
- Classificatie vertrouwelijkheid (waarden Laag, Midden, Hoog)
- Classificatie privacy (waarden Laag, Midden, Hoog)
- Classificatie duurzame toegankelijkheid (waarden Laag, Midden, Hoog)
- Basisbeveiligingsniveau (waarden BBN1, BBN2, BBN2+[3])

De i-Navigator bevat voor elk van deze classificaties twee velden: een modelveld dat centraal wordt beheerd door de redactie en een lokaal veld dat kan worden aangepast door de lokale beheerder.

Informatiesystemen

De bovengenoemde velden zijn ook toegevoegd voor informatiesystemen. Omdat informatiesystemen echter niet centraal worden beheerd door de redactie zijn in dit onderdeel alleen de lokale velden toegevoegd. Het is echter relatief eenvoudig om deze velden te vullen wanneer de informatiesystemen zijn gekoppeld aan registraties: een classificatie van een informatiesysteem komt overeen met de hoogste classificatie van de gekoppelde registraties. Dus: wanneer bijvoorbeeld het informatiesysteem ‘Money4Nothing’ is gekoppeld aan de registraties ‘Financiën’ en ‘Subsidies’ waarbij de eerste Midden scoort op Vertrouwelijkheid en de tweede Hoog, dan krijgt Money4Nothing de waarde Hoog.

Waarden

Door toevoeging van BBN2+ heeft de classificatie ‘Hoog’ een andere lading gekregen. Bovendien heeft de IBD een andere classificatie geïntroduceerd die uit 4 waarden bestaat, onder de waarde ‘Laag’ is nog een waarde toegevoegd voor Beschikbaarheid, Integriteit en Vertrouwelijkheid. Op basis hiervan hebben wij onze regels opnieuw gewaardeerd, we hebben daarbij de volgende afweging gemaakt:

- Voor Beschikbaarheid wordt in de BIO naast de waarde ‘Laag’ soms ook de waarde ‘Niet zeker’ gebruikt. Vanwege slechte operationaliseerbaarheid van dit begrip hebben wij deze waarde gelijkgesteld met de waarde ‘Laag’.
- Voor Integriteit wordt in de BIO naast de waarde ‘Laag’ soms ook de waarde ‘Verwaarloosbaar’ gebruikt. Vanwege slechte operationaliseerbaarheid van dit begrip hebben wij deze waarde gelijkgesteld met de waarde ‘Laag’.
- Voor Vertrouwelijkheid wordt in de BIO naast de waarde ‘Laag’ soms ook de waarde ‘Openbaar’ gebruikt. Vanwege slechte operationaliseerbaarheid van dit begrip hebben wij deze waarde gelijkgesteld met de waarde ‘Laag’.

3.2 De gehanteerde werkwijze

Zoals eerder vermeld heeft de ‘standaardaanpak’ op basis van workshops twee tekortkomingen: (i) het is niet mogelijk alle processen en informatiesystemen mee te nemen dus men beperkt zich tot de ‘usual suspects’ en (ii) er zijn grote inconsistenties in de uitkomsten te verwachten. Onze gehanteerde werkwijze is er dan ook op gericht deze problemen te voorkomen.

Om inconsistenties te voorkomen is begonnen met het opstellen van algemene regels op basis waarvan alle processen kunnen worden geclassificeerd. Deze regels zijn gebaseerd op een analyse uit de volgende bronnen:

- Handreiking dataclassificatie BIO, IBD, versie 2.1, augustus 2019.
- Dataclassificatietoets BIO gemeenten, IBD, versie 1.2, januari 2021.

[3] Het BBN3-niveau is hier buiten beschouwing gelaten, aangezien dit niveau niet van toepassing is voor gemeenten.

- Baseline Informatiebeveiliging Overheid (BIO), versie 1.04, 4 november 2019.
- Baselinetoets BBN-BIO, IBD versie 1.02, mei 2019.
- Maatregelenset BBN2+, IBD, versie 1.01, augustus 2020.
- Handreiking Diepgaande Risicoanalyse Methode Gemeenten, versie 2.1.
- Diepgaande Risicoanalyse Methode Gemeenten, Versie 2.1.
- Schadescenario's BBN2+, versie 0.9.
- Privacy Impact Assessment (PIA) introductie, handreiking en vragenlijst, Norea, versie 1.2, november 2015.
- Vragenlijst PIA, IBD, versie 1.0, april 2014.
- Handreiking Kwaliteitssysteem Informatiebeheer Decentrale Overheden (KIDO), versie 1.0, 29 november 2016.
- Selectielijst gemeenten en intergemeentelijke organen 2020, Staatscourant 11143 van 26 februari 2020.

Deze regels zijn geoperationaliseerd tot 'objectief' vast te stellen eigenschappen van de processen en registraties. Waar mogelijk is hierbij gebruik gemaakt van gegevens die al onderdeel uitmaken van het model-DSP. Om een eenvoudig voorbeeld te geven: de regel '*De PIA-waarde is Hoog als er bijzondere persoonsgegevens verwerkt kunnen worden in een proces'* kan direct worden afgeleid uit de AVG metadata die al onderdeel vormen van het model-DSP.

Vervolgens zijn de regels toegepast op alle processen in de model-DSP's om de BIV-, privacy- en duurzame toegankelijkheidsclassificaties vast te stellen. De BIV-classificaties zijn vervolgens vertaald naar BBN waarderingen op basis van de richtlijnen uit de dataclassificatietoets BIO gemeenten (IBD).

De laatste stap was het classificeren van de model-DSP registraties. Hierbij is de volgende regel toegepast: Een registratie krijgt voor alle classificaties (beschikbaarheid, integriteit, vertrouwelijkheid, privacy en BBN) de hoogste classificatie van de aan de registratie gekoppelde processen. Een gevolg hiervan is dat een registratie nooit een lagere classificatie heeft dan een gekoppeld proces.

3.3 Conclusie

Door de gehanteerde werkwijze is een consistente en complete model-risicoclassificatie gemaakt wat als uitgangspunt kan dienen voor model-DSP klanten. Uiteraard blijft het een model en zal in uw eigen organisatie moeten worden nagegaan waar wordt afgeweken van het model. Het betekent echter dat de CISO, Privacy officer of Informatiemanager een basis heeft waarop hij of zij kan voortborduren en het geeft u een startpunt dat verder ligt dan wat u anders ooit als eindpunt had kunnen bereiken.

Het inzicht dat de risicoclassificatie u oplevert is een eerste stap naar het op orde krijgen van de informatiebeveiliging. Op basis hiervan dient u vast te stellen welke risico's aanvaardbaar zijn en welke er moeten worden afgedekt. Voor het afdekken van risico's zullen passende maatregelen genomen moeten worden. Geschikte maatregelen zijn onder andere te vinden in de BIO, de ISO 27001/2, de Privacy Baseline en KIDO.

Uiteraard valt of staat de kwaliteit van de model-risicoclassificatie met de kwaliteit van de toegepaste regels. Daarom zijn bij wijze van verantwoording deze regels toegelicht in de volgende sectie.

4. Verantwoording

In deze sectie hebben we per toegepaste classificatie (Beschikbaarheid, Integriteit, Vertrouwelijkheid, BBN, Privacy en Duurzame toegankelijkheid) de gehanteerde regels en operationalisaties beschreven.

4.1 Beschikbaarheid

Met beschikbaarheid wordt aangegeven in hoeverre data of een informatiesysteem voor de gebruiker toegankelijk moet zijn en gebruikt moet kunnen worden op het moment dat dit nodig is. Dit wordt in het model-DSP aangegeven aan de hand van de waarden Laag, Midden en Hoog. Deze waarden worden ook in de Baseline

Informatiebeveiliging Overheid (BIO) gebruikt om de Basisbeveiligingsniveaus te definiëren. Daarnaast worden in de BIO de waarden de waarden Essentieel, Noodzakelijk, Belangrijk en Niet zeker gebruikt om het beschikbaarheidsniveau te definiëren. Wij hebben er voor gekozen om overal te werken met de generieke waarden Laag, Midden en Hoog die wij vertaald hebben naar de in de BIO gehanteerde waarden. Aan de waarden is de volgende betekenis gegeven:

- **Laag** (BIO: Belangrijk, Niet zeker): Het informatiesysteem mag incidenteel uitvallen voor maximaal twee weken (ook in piekperiodes) en dit heeft nauwelijks of geen gevolgen voor burgers/gebruikers.
- **Midden** (BIO: Noodzakelijk)**:** : Het informatiesysteem mag beperkt korte tijd uitvallen voor maximaal één week (ook in piekperiodes) en dit heeft voelbare gevolgen voor burgers/gebruikers.
- **Hoog** (BIO: Essentieel): Het informatiesysteem mag slechts in uitzonderlijke situaties uitvallen en dient zo snel mogelijk weer hersteld te worden. Uitval heeft (zeer) grote gevolgen voor burgers/gebruikers.

Regels

De volgende regels zijn gebruikt om het beschikbaarheidsniveau van processen in het model-DSP te bepalen:

1.1 Als een proces uitgevoerd wordt bij het optreden van een ramp of calamiteit is het Beschikbaarheidsniveau ‘Hoog’.

Wanneer er sprake is van een ramp of calamiteit is het van groot belang dat benodigde informatie direct voorhanden is. Het niet beschikbaar zijn van essentiële informatie om juist en tijdig te handelen bij een calamiteit of ramp kan tot (zeer) grote gevolgen leiden.

In het model-DSP voor Gemeenten zijn door de redactie de volgende processen geïdentificeerd die uitgevoerd worden bij het optreden van een ramp of calamiteit:

- Rampenbestrijding
- Calamiteit afhandeling systeem of applicatie
- Vondst explosiefmelding
- Noodverordening opstelling
- Noodbevel opstelling

1.2 Als bij een proces direct moet worden gereageerd op een plotselinge gebeurtenis is het Beschikbaarheidsniveau ‘Hoog’.

Wanneer er snel gehandeld moet worden is het van cruciaal belang dat de benodigde informatie ook direct beschikbaar is. Het niet beschikbaar zijn van de benodigde informatie kan leiden tot het niet op tijd reageren en daarmee tot (zeer) grote gevolgen.

De volgende processen in het model-DSP zijn door de redactie vastgesteld als processen waarbij een snelle reactie noodzakelijk is:

- Processen waar uit de naam of de omschrijving van het proces blijkt dat het een spoedeisend proces is.
- Processen waarvan de binnenkomende meldingen direct door de organisatie moeten worden opgepakt.
- Processen die worden getriggerd door een spoedeisende melding van een ketenpartner

1.3 Als een proces leidt tot mutaties in de burgerlijke stand (geboorte en overlijden) is het Beschikbaarheidsniveau ‘Hoog’.

Mutaties in de burgerlijke stand moeten binnen drie dagen zijn gemeld en verwerkt (Besluit Burgerlijke Stand 1994). Om de mutaties binnen deze termijn te kunnen verwerken is het van belang dat de hiervoor benodigde informatie(systemen) beschikbaar zijn. In het model-DSP voor Gemeenten zijn dit de processen inzake aangifte geboorte en overlijden.

1.4 Als het niet beschikbaar zijn van het resultaat van een uitgevoerd proces, kan leiden tot gevaar voor de gezondheid of het welzijn van personen of tot grote maatschappelijke gevolgen, is het Beschikbaarheidsniveau 'Hoog'.

Er dient te allen tijde voorkomen te worden dat het niet beschikbaar zijn van informatie gevaar oplevert voor burgers. Daarom is voor alle processen waar dit het geval zou kunnen zijn de waarde voor Beschikbaarheid op 'Hoog' gezet. Omdat het hier om voorbereidende processen gaat, is het enkel van belang dat het resultaat van dit proces beschikbaar is, de informatie die tot dit resultaat heeft geleid is niet noodzakelijk om tijdig te kunnen reageren. In het model-DSP vallen in elk geval de volgende processen onder deze categorie:

- Opstellen rampenplan, crisisbeheersingsplan
- Opstelling uitwijkplan
- Continuïteitsplan
- Intern calamiteitenplan
- De werkprocessen die registraties Milieu-inrichting of Risicosituaties gevaarlijke stoffen muteren
- Veiligheidsrapporten milieu-inrichtingen
- Waterstand/omgevingswaarde monitoring
- BRZO-rapporten
- Vergunningen / meldingen m.b.t. vuurwerk
- Evenementenvergunning/melding/ontheffing
- Betoging melding
- Agressie tegen personeelslid
- Arbo-incident
- Gladheidsbestrijdingsplan
- Dijkbewaking uitvoering
- Toezicht infectieziekten
- Vaccinatie verstrekking

1.5 Als een intern proces de uitvoering van één of meerdere reactieve processen (1.1, 1.2) met beschikbaarheid 'Midden/Hoog' kan blokkeren, dan is het Beschikbaarheidsniveau 'Midden/'Hoog'

Interne processen kunnen informatie bevatten die nodig is voor de uitvoering van primaire processen. Als het interne proces noodzakelijk is voor een primair proces en het niet beschikbaar zijn van dit interne proces niet makkelijk via een alternatieve methode kan worden opgelost, blokkeert het interne proces de uitvoering van het primaire proces. Het interne proces krijgt daarom hetzelfde beschikbaarheidsniveau als het gerelateerde primaire proces.

1.6 Als het niet beschikbaar zijn van informatie leidt tot een ernstig verlies van management control, is het beschikbaarheidsniveau 'Hoog'

We hebben deze regel vooral toegepast op die werkprocessen die erop gericht zijn om geaccumuleerde informatie aan te leveren waar managementbeslissingen en/of beleidskeuzes op gebaseerd worden, zoals de processen Interne audit, Rapportage periodiek intern en Rapportage periodiek Extern.

1.7 Als het niet beschikbaar zijn van informatie vertraging van nieuwe ontwikkelingen tot gevolg heeft, 'Hoog'

Met 'nieuwe ontwikkelingen' kan bijvoorbeeld gedacht worden aan de realisatie van beleidsambities die per organisatie kunnen verschillen. Deze regel kan dan ook als zodanig niet worden opgenomen in het model-DSP omdat het hier maatwerk betreft.

1.8 Als het niet beschikbaar zijn van informatie in een proces kan leiden tot het niet behalen van wettelijke afdoeningstermijnen en daarmee tot juridische of financiële aansprakelijkheid is het beschikbaarheidsniveau 'Midden' of 'Laag', afhankelijk van de afdoeningstermijn.

Voor processen met een afdoeningstermijn van meer dan 2 weken geldt dat het minder erg is als informatie voor bepaalde tijd niet beschikbaar is dan voor processen die binnen 2 weken afgehandeld moeten worden. Een langere afdoeningstermijn biedt immers meer mogelijkheden om het proces op een later moment af te handelen zonder dat dit direct gevolgen heeft. Daarom is voor processen met een afdoeningstermijn van 2 weken of minder de waarde voor Beschikbaarheid 'Midden' en voor processen met een afdoeningstermijn van meer dan 2 weken 'Laag'.

1.9 Als het niet beschikbaar zijn van informatie in een proces zou kunnen leiden tot het niet kunnen nakomen van contractuele verplichtingen is het beschikbaarheidsniveau 'Midden' [4]

Indien een organisatie taken uitvoert voor een andere organisatie dienen er afspraken gemaakt te zijn over servicelevels en afdoeningstermijnen. Wanneer informatie die nodig is om deze taken uit te voeren niet beschikbaar is kan de organisatie haar contractuele verplichtingen niet nakomen. De ernst van het niet kunnen nakomen van verplichtingen is afhankelijk van de inhoud van de overeenkomst en het uit te voeren proces. Deze regel is relevant voor processen die de organisatie uitvoert voor een andere organisatie en waar geen wettelijke afdoeningstermijnen voor zijn vastgelegd (wanneer deze er wel zijn valt het proces onder regel 1.6).

1.10 Als een proces niet onder één van bovenstaande regels valt, is het beschikbaarheidsniveau 'Laag'.

4.2 Integriteit

Met integriteit wordt aangegeven in hoeverre informatie juist, volledig, actueel en (ongeoorloofd) ongewijzigd is. Integriteitsissues kunnen uiteindelijk leiden tot verkeerde besluiten of uitkomsten van een proces. De impact van een integriteitsissue is dan ook gelijk te stellen aan de impact van een verkeerd besluit.

Integriteit wordt in het model-DSP aangegeven aan de hand van de waarden Laag, Midden en Hoog. Deze waarden worden ook in de Baseline Informatiebeveiliging Overheid (BIO) gebruikt om de Basisbeveiligingsniveaus te definiëren. Daarnaast worden in de BIO de waarden Desastreus, Ernstig, Gering en Verwaarloosbaar gebruikt om het integriteitsniveau te definiëren. Wij hebben er voor gekozen om te blijven werken met de generieke waarden Laag, Midden en Hoog die wij vertaald hebben naar de in de BIO gehanteerde waarden. Aan de waarden is de volgende betekenis gegeven:

- **Laag** (Gering, Verwaarloosbaar): Er zijn geen bijzondere maatregelen noodzakelijk om de juistheid, tijdigheid en volledigheid van informatie te waarborgen (VIR definitie). Het verlies van integriteit kan leiden tot beperkte schade.[5]
- **Midden** (Ernstig): Er zijn passende maatregelen noodzakelijk om de juistheid, tijdigheid en volledigheid van informatie (VIR definitie) te waarborgen. Het verlies van integriteit kan leiden tot forse schade.
- **Hoog** (Desastreus): Er zijn zware maatregelen noodzakelijk om de integriteit van informatie te waarborgen. Het verlies van integriteit kan leiden tot zware schade.

Regels

De volgende regels zijn gehanteerd voor het bepalen van het Integriteitsniveau in het model-DSP:

[4] Deze regel is gebaseerd op informatie die niet op model-niveau beschikbaar is. Daarom is deze niet toegepast in de model-risicoclassificaties in het model-DSP.

2.1 Als een proces muteert in een basisregistratie c.q. landelijke registratie waar gegevens worden opgeslagen, is het integriteitsniveau 'Hoog'

Wanneer als gevolg van integriteitsverstoringen in een proces verkeerde (dat wil zeggen niet integere) informatie terecht komt in basisregistraties c.q. landelijke registratie waar gegevens worden opgeslagen kan dit grote gevolgschade veroorzaken die bovendien moeilijk herstelbaar is.

2.2 Als in een proces financiële transacties plaats vinden is het Integriteitsniveau 'Midden'.

Wanneer er onjuiste transacties gedaan worden op basis van niet integere informatie, levert dit financiële gevolgen op voor de organisatie. Afhankelijk van de grootte en/of de frequentie van de transactie(s) kan dit flinke schade opleveren.

Processen waarin financiële transacties plaats vinden zijn in het model-DSP te herkennen doordat zij gekoppeld zijn aan de registratie *Financiën* én er sprake is van een mutatie in die registratie.

2.3 Als een proces tot een besluit of beschikking leidt met een financiële transactie (m.u.v. leges) tot gevolg is het Integriteitsniveau 'Midden'.

Wanneer in een proces dat leidt tot een financiële transactie verkeerde besluiten worden genomen, dan leidt dit tot financiële schade voor de organisatie. Dit kan voorkomen worden door maatregelen te nemen om de integriteit van de informatie in het betreffende proces te verhogen.

Alle processen in het model-DSP met het documenttype *Besluit, Beschikking, of Uitspraak* zijn door de redactie langsgelopen om te bepalen of er een financiële transactie plaats vindt. Ook binnenkomende besluiten en beschikkingen die leiden tot financiële transacties vallen onder deze regel.

2.4 Als een proces leidt tot een besluit of beschikking met schadelijke en/of moeilijk te herstellen gevolgen is het Integriteitsniveau 'Midden'.

Wanneer de gevolgen van een verkeerd besluit niet of moeilijk te herstellen zijn, heeft een verkeerd besluit een veel grotere impact op een organisatie dan wanneer een besluit eenvoudig terug te draaien is. Om de processen waarbij dit het geval is aan te duiden in het model-DSP, heeft de redactie alle processen met het documenttype *Besluit* of *Beschikking* langsgelopen en per proces bepaald of er sprake is (of kan zijn) van schadelijke en/of moeilijk te herstellen gevolgen.

2.5 Als een proces politieke of maatschappelijke impact kan hebben is het Integriteitsniveau 'Midden'.

Een proces met politieke of maatschappelijke impact kan, indien niet uitgevoerd op basis van integere informatie, onder andere leiden tot forse politieke of imagoschade.

Om te bepalen welke processen onder deze categorie vallen heeft de redactie alle processen die geïnitieerd worden door een burger of organisatie (met kenmerk *Trigger Extern* in het model-DSP) nagelopen. Van deze selectie zijn de processen met externe werking aangewezen als processen waarin mogelijk sprake kan zijn van politieke of maatschappelijke impact. Processen waarbij de initiator een overheidsinstelling in 'de keten' is, zijn hierbij uitgesloten.

2.6 Als onjuiste informatie in een proces gericht op managementcontrole, leidt tot onjuiste managementbeslissingen en of/beleidskeuzes, is het integriteitsniveau 'Midden'

We hebben deze regel vooral toegepast op die werkprocessen die erop gericht zijn om geaccumuleerde informatie aan te leveren waar managementbeslissingen en/of beleidskeuzes op gebaseerd worden, zoals de processen Interne audit, Rapportage periodiek intern en Rapportage periodiek Extern.

4.7 Als een proces niet onder één van bovenstaande regels valt, is het integriteitsniveau ‘Laag’.

4.3 Vertrouwelijkheid

Bij Vertrouwelijkheid gaat het erom dat bevoegdheden en de mogelijkheden tot muteren, kopiëren, toevoegen, vernietigen of kennisnemen van informatie beperkt zijn tot de hiertoe aangewezen personen.

De BIV-classificatie voor Vertrouwelijkheid wordt in het model-DSP aangegeven aan de hand van de waarden Laag, Midden en Hoog. Deze waarden worden ook in de Baseline Informatiebeveiliging Overheid (BIO) gebruikt om de Basisbeveiligingsniveaus te definiëren. Daarnaast worden in de BIO de waarden Geheim, Vertrouwelijk, Intern en Openbaar gebruikt om het vertrouwelijkheidsniveau te definiëren. Wij hebben er voor gekozen om overal te werken met de generieke waarden Laag, Midden en Hoog die wij vertaald hebben naar de in de BIO gehanteerde waarden. Aan de waarden is de volgende betekenis gegeven:

De gebruikte niveaus van vertrouwelijkheid zijn:

- **Laag** (BIO: Intern, Openbaar): Organisatievertrouwelijk - Kennisname van informatie door niet-geautoriseerden (buitenstaanders) is niet gewenst, maar leidt niet tot schade van enige omvang.
- **Midden** (BIO: Vertrouwelijk): Afdelingsvertrouwelijk - Bescherming van gegevens en andere te beschermen belangen in de processen van de overheid, waar o.a. vertrouwelijkheid aan de orde is, omdat het om gevoelige informatie gaat.
- **Hoog** (BIO: Geheim): Behandelaarvertrouwelijk - De toegang van informatie moet worden beperkt tot die groep van mensen die voor het juist uitvoeren van hun werkzaamheden afhankelijk zijn van deze informatie.

Regels

De volgende regels zijn gehanteerd om het vertrouwelijkheidsniveau van processen te bepalen:

3.1 Als een proces vertrouwelijke informatie bevat die voor alle medewerkers van de organisatie (die geen behandelaar van het proces zijn) moet worden afgeschermd is het Vertrouwelijkheidsniveau ‘Hoog’.

Het gaat hier om processen die zeer vertrouwelijke informatie bevatten, waarbij het van belang is dat deze informatie alleen toegankelijk is voor degenen die hier daadwerkelijk iets mee moeten doen en hiertoe geautoriseerd zijn. Verlies van dergelijke informatie heeft een grote impact.

In het algemeen gaat het om de volgende specifieke processen:

- Klokkenluidersmelding
- Integriteitsonderzoek
- (Koninklijke) onderscheiding
- Klacht ongewenst gedrag
- Loonbeslaglegging
- Organisatiewijziging
- Fraude meldingen
- Opsporing overtreder
- Proces verbaal
- Processen omtrent het benoemen, en ontslaan van bestuurders (burgemeester, dijkgraaf, commissaris van de koning, algemeen directeur en bestuurders van onderwijsinstellingen en woningcorporaties)

In het model-DSP voor Gemeenten gaat het om de volgende specifieke processen:

- Processen omtrent het ontslaan van wethouders en raadsleden

In het model-DSP voor Waterschappen gaat het om de volgende specifieke processen:

- Processen omtrent het ontslaan van heemraden en leden van het Algemeen Bestuur

In het model-DSP voor Onderwijsinstellingen gaat het om de volgende specifieke processen:

- het schorsen en ontslaan van hoogleraren, lectoren en docenten
- het benoemen van lectoren en hoogleraren
- Het toekennen van eredoctoraten
- Het verlenen van graden

In het model-DSP voor Provincie gaat het om de volgende specifieke processen:

- Processen omtrent het ontslaan leden van de Provinciale Staten

In het model-DSP voor Veiligheidsregio's gaat het om de volgende specifieke processen:

- Processen omtrent het benoemen, en ontslaan van bestuurders (voorzitter, bestuursleden, bestuurscommissieleden)

3.2 Als er contractuele of wettelijke verplichtingen zijn die Vertrouwelijkheid Midden/Hoog vereisen dan Vertrouwelijkheid Midden/Hoog.

Processen waarin gegevens worden verwerkt waar de organisatie vanuit contractuele of wettelijke verplichtingen vertrouwelijk mee om moet gaan, krijgen een vertrouwelijkheidsniveau dat aansluit bij die contractuele of wettelijke verplichtingen.

Voorbeeld: de Basisregistratie Personen moet, wettelijk gezien, worden afgeschermd op afdelingsniveau en krijgt daarom het Vertrouwelijkheidsniveau 'Midden'.

3.3 Als in een proces bijzondere persoonsgegevens of het BSN verwerkt worden is het Vertrouwelijkheidsniveau 'Midden'.

Bijzondere persoonsgegevens en het BSN gelden als gevoelige informatie. Openbaar worden van deze informatie kan leiden tot schade op verschillende gebieden.

Processen met bijzondere persoonsgegevens zijn in het model-DSP te identificeren door middel van het veld *Soort persoonsgegevens* op het tabblad AVG (m).

Voor wat betreft het BSN geldt deze regel alleen voor werkprocessen waarbij het BSN tijdens het uitvoeren van het werkproces ook daadwerkelijk gebruikt wordt, niet voor werkprocessen waarbij het BSN op de achtergrond gebruikt wordt in de koppeling met de BRP om bijvoorbeeld afzendergegevens op te halen. Binnen de processen waarin het BSN gebruikt wordt (in het model-DSP te identificeren door middel van het veld *Soort persoonsgegevens* op het tabblad AVG (m)) is door de redactie een handmatige selectie gemaakt van processen waarbij het BSN actief gebruikt wordt om een wijziging door te voeren in een (basis)registratie.

3.4 Als een proces informatie bevat waarmee ongeautoriseerde toegang tot systemen kan worden verkregen is het Vertrouwelijkheidsniveau 'Midden'.

Wanneer ongeautoriseerde personen toegang krijgen tot informatie(systemen) kan dit ertoe leiden dat gevoelige, vertrouwelijke informatie openbaar wordt. Dit kan voor de organisatie voor forse schade zorgen.

In het model-DSP zijn dit bijvoorbeeld de processen rondom het uitgeven van accounts van systemen.

3.5 Als een proces vertrouwelijke informatie bevat waarmee in geval van bekendwording identiteitsfraude kan worden gepleegd is het Vertrouwelijkheidsniveau 'Midden'.

Het gaat hier om processen waarbij bijvoorbeeld een kopie van een identiteitsbewijs is opgeslagen. Wanneer deze informatie in verkeerde handen terechtkomt, kan dit leiden tot behoorlijke schade door bijvoorbeeld identiteitsfraude.

In het model-DSP zijn processen waarin een kopie van een identiteitsbewijs wordt opgeslagen te herkennen aan de aanwezigheid van een documenttype van het documentsoort *Bewijs identiteit*.

3.6 Als een proces vertrouwelijke informatie bevat waarmee door bekendwording met voorkennis gehandeld kan worden is het Vertrouwelijkheidsniveau 'Midden'.

Het handelen met voorkennis door onterecht verkregen vertrouwelijke informatie (door derden) kan leiden tot forse schade voor de organisatie, zowel financieel als politiek en/of maatschappelijk.

Dit is in het model-DSP het geval bij processen met als onderwerp *Ruimtelijke plannen* en het vestigen van een voorkeursrecht. In het provinciaal DSP betreft het tevens processen die vertrouwelijke informatie bevatten van proces-/productinformatie van milieu-inrichtingen.

3.7 Als een proces vertrouwelijke informatie bevat over aankoop-, verkoop- of inkoopcontracten is het Vertrouwelijkheidsniveau 'Midden'.

Dergelijke contracten kunnen (vertrouwelijke) informatie bevatten die de organisatie schade kan berokkenen bij bekendwording hiervan.

In het model-DSP vallen alle processen met als onderwerp *Aankoop*, *Verkoop, Huur, Verhuur, Verpachting, Inkoop*, *Contract* of *Uitgifte*[6] hier onder.

3.8 Als een proces vertrouwelijke informatie bevat die kan leiden tot aansprakelijkstelling op basis van wettelijke of contractuele verplichtingen is het Vertrouwelijkheidsniveau 'Midden'.[7]

Wanneer bekendwording van vertrouwelijke informatie leidt tot een aansprakelijkstelling kan dit de organisatie behoorlijke schade opleveren.

Concreet gaat het hier in het model-DSP om alle processen die een documenttype van het documentsoort *Overeenkomst* bevatten, waarbij de overeenkomst een geheimhoudingsclausule kan bevatten.

3.9 Als een proces vertrouwelijke informatie bevat over personeelszaken of studentenzaken is het Vertrouwelijkheidsniveau 'Midden'.

Processen met betrekking tot personeelszaken bevatten over het algemeen vertrouwelijke informatie. Onder deze categorie vallen de processen in het model-DSP met als taakveld *Personeelszaken* die betrekking hebben op individuele personeelsleden. Processen die betrekking hebben op de adviserende rol van de Ondernemingsraad vallen ook onder deze regel. In het model-DSP voor Onderwijs vallen hier tevens de processen met vertrouwelijke informatie over studenten onder.

3.10 Als een proces informatie verwerkt over individuele cliënten binnen het Sociale domein is het Vertrouwelijkheidsniveau 'Midden'.

[6] Ook 'Ruiling', 'Onteigening' en 'Verjaring' vallen onder deze regel

[7] Deze regel is niet toegepast bij de model-risicoclassificaties in het model-DSP omdat toepassing ervan zaakspecifieke informatie vraagt.

Het gaat hier om processen waarin persoonsgegevens over cliënten worden verwerkt.

3.11 Als een proces betrekking heeft op een bestuursrechtelijke overtreding is het Vertrouwelijkheidsniveau ‘Midden’.

Processen met betrekking tot bestuursrechtelijke overtredingen bevatten vertrouwelijke gegevens die schadelijk kunnen zijn bij openbaarmaking.

De volgende processen in het model-DSP hebben in elk geval betrekking op een bestuursrechtelijke overtreding:

- Bestuurlijke boete overlast in de openbare ruimte
- Bestuurlijke strafbeschikking

In het Gemeentelijk Model-DSP geldt dit tevens voor de volgende werkprocessen:

- Handhaving door gemeente
- Handhavingsbeschikking [Omgevingswet]
- Last onder bestuursdwang ten uitvoer legging [Omgevingswet]
- Last onder dwangsom ten uitvoer legging [Omgevingswet]

In het Model-DSP voor Waterschappen geldt dit tevens voor:

- Handhaving door waterschap
- Proces verbaal opstelling
- Boeterapport
- Handhaving Bestuursdwang
- Handhaving Last onder dwangsom
- Last onder bestuursdwang ten uitvoer leggen (omgevingswet)
- Last onder dwangsom ten uitvoer legging (omgevingswet)

In het Model-DSP voor Provincies geldt dit tevens voor:

- Handhaving door provincie
- Handhavingsbesluit nemen (omgevingswet)
- Proces verbaal
- Bestuurlijke boete omgevingsrecht
- Last onder bestuursdwang ten uitvoer legging [Omgevingswet]
- Last onder dwangsom ten uitvoer legging [Omgevingswet]

In het Model-DSP voor Veiligheidsregio’s geldt dit tevens voor:

- Handhaving door veiligheidsregio
- Handhavingsbeschikking [Omgevingswet]
- Last onder bestuursdwang ten uitvoer leggen [Omgevingswet]
- Last onder dwangsom ten uitvoer legging [Omgevingswet]

3.12 Als een proces vertrouwelijke informatie bevat over de totstandkoming van beleid is het Vertrouwelijkheidsniveau ‘Midden’.

In uitzonderlijke gevallen is beleid of voorbereiding ervan vertrouwelijk maar deze zaaktypen zijn niet afzonderlijk herkenbaar in het model-DSP.

3.13 Als bekendwording van vertrouwelijke informatie binnen een proces leidt tot een ondermijning van de openbare orde en veiligheid, is het vertrouwelijkheidsniveau 'Midden'.

Het verlies van vertrouwelijke informatie kan een zeer schadelijk effect hebben op de handhaving van de openbare orde waardoor taken niet meer uitgevoerd kunnen worden.

Voor het model-DSP voor gemeenten heeft de redactie vastgesteld dat deze regel betrekking heeft op de volgende processen:

- Evenementenvergunning
- Noodbevel opstelling
- Noodverordening opstelling
- Ondermijnende criminaliteit melding
- Politiegegevens verstrekking verzoek
- Radicalisering melding
- Rampenbestrijding
- Veiligheidsrisicogebied aanwijzingsbesluit

3.14 Als een proces informatie bevat die leidt tot een ondermijning van de democratische besluitvorming is het vertrouwelijkheidsniveau 'Midden'

De vertrouwelijkheid van informatie is essentieel voor de werking van het democratische proces. Wanneer dit wordt geschonden kunnen de consequenties voor de maatschappij zeer groot zijn. Denk bijvoorbeeld aan het aftreden van een regering of een schending van het stemproces doordat vertrouwelijke gegevens op straat komen te liggen.

Voor het model-DSP voor gemeenten heeft de redactie vastgesteld dat deze regel betrekking heeft op de volgende processen:

- Bestuurlijke besluitvorming
- Enquête door gemeenteraad
- Kiesrechtuitsluiting
- Stemmen per brief
- Verkiezing
- Vervangende stempas
- Volmacht bewijs stemmen

3.15 Als een proces niet onder één van bovenstaande regels valt, is het vertrouwelijkheidsniveau 'Laag'.

4.4 Basisbeveiligingsniveau

De BIO definieert vier Basisbeveiligingsniveaus (BBN's) waarmee het risicomanagement afgestemd kan worden op de te beschermen belangen en relevante dreigingen. Daardoor hoeven organisaties alleen maatregelen door te voeren die gelden voor het BBN dat voor de betreffende informatie is vastgesteld. De basisbeveiligingsniveaus zijn globaal als volgt ingedeeld:

- **BBN1**: 'Wat mag minimaal verwacht worden?'. Dit niveau geldt voor informatie waarbij de niveaus voor beschikbaarheid, integriteit en vertrouwelijkheid de waarde Laag hebben.
- **BBN2**: Bescherming van de meest voorkomende categorieën informatie. Dit niveau geldt voor informatie waarbij de niveaus voor beschikbaarheid, integriteit en vertrouwelijkheid de waarde Midden hebben.
- **BBN2+**: Wanneer beschikbaarheid, vertrouwelijkheid of integriteit de waarde 'Hoog' hebben, zijn wellicht extra maatregelen nodig boven het standaard BBN2 niveau. BBN2+ geeft de mogelijkheid om (op basis van een nadere risicoanalyse) indien nodig additionele maatregelen te treffen.
- **BBN3**: Bescherming van informatie met de rubricering Departementaal Vertrouwelijk of vergelijkbaar, waarbij weerstand tegen statelijke actoren of vergelijkbare dreigers nodig is. Dit niveau geldt voor

informatie waarbij de niveaus voor beschikbaarheid en integriteit de waarde Midden hebben en het niveau voor vertrouwelijkheid de waarde Hoog.

Het BBN is ook opgenomen in het model-DSP en wordt vastgesteld op basis van de toegekende BIV-waarden. Hierbij zijn de volgende regels gehanteerd:

- Wanneer Beschikbaarheid, Integriteit en Vertrouwelijkheid Laag zijn geldt BBN1.
- BBN2+ geldt indien de Beschikbaarheid en/of Integriteit en/of Vertrouwelijkheid Hoog is.
- In alle andere gevallen geldt BBN2.

BBN3 wordt niet toegekend in het model-DSP, aangezien dit niveau niet van toepassing is op lagere overheden.

4.5 PIA-inventarisatie

Naast het inventariseren van de niveaus voor Beschikbaarheid, Integriteit en Vertrouwelijkheid is ook het inventariseren van de risico's op het gebied van privacy meegenomen in het model-DSP. Dit is de Privacy Impact Assessment (PIA). De redactie heeft aan de hand van de PIA-vragenlijst (NOREA) geïnventariseerd welke factoren leiden tot een verhoogd risico. Hierbij zijn de volgende risicowaarden gehanteerd:

- **Laag**: er is sprake van weinig tot geen risico op het gebied van privacy
- **Midden**: er is sprake van een gemiddeld risico op het gebied van privacy
- **Hoog**: er is sprake van een verhoogd risico op het gebied van privacy

Aan de hand van de lijst van factoren uit de NOREA-vragenlijst zijn een aantal regels opgesteld die gebruikt zijn bij het bepalen van de PIA-waardering van de processen in het model-DSP. Deze lijst is terug te vinden onder het kopje 'Toegepaste regels en operationalisatie'. Praktisch gezien leidt toepassing van deze regels echter tot onderstaande basisregels.

De basisregels zijn:

- **De PIA-waarde is Hoog als er bijzondere persoonsgegevens verwerkt kunnen worden in een proces.**
- **De PIA-waarde is Midden als er basispersoonsgegevens verwerkt kunnen worden in een proces.**
- **De PIA-waarde is Laag als er geen persoonsgegevens verwerkt worden in een proces.**

Regels

De volgende regels geven een aanvulling op bovenstaande basisregels of dienen als verdere verantwoording hiervan:

4.1 Als er wet- en regelgeving is die als grondslag kan worden gebruikt of die het expliciet toestaat om bijzondere persoonsgegevens te verwerken in het betreffende proces is de PIA-waarde 'Hoog'.

Deze regel dekt de factor 'Grote hoeveelheid wet- en regelgeving ten aanzien van persoonsgegevens die verwerkt worden'. Het is echter lastig aan te duiden wanneer er sprake is van 'grote hoeveelheid wet- en regelgeving', daarom is er hier uitgegaan van alle processen waarvoor wet- en regelgeving geldt met betrekking tot persoonsgegevens die verwerkt worden.

4.2 Als in een proces persoonsgegevens worden verkregen van of verstrekt aan een ketenpartner dan geldt een verhoogd risico. Hierbij wordt onderscheid gemaakt tussen basispersoonsgegevens en bijzondere persoonsgegevens.

- **Bij verwerking van basispersoonsgegevens is de PIA-waarde 'Midden'.**
- **Bij verwerking van bijzondere persoonsgegevens is de PIA-waarde 'Hoog'.**

Het uitwisselen van persoonsgegevens met een ketenpartner is een indicatie dat er veel maatschappelijke belanghebbenden zijn of dat er veel partijen betrokken zijn bij de uitvoering van het project/proces. Dit zorgt voor een verhoogd privacyrisico.

4.3 Als een proces meer dan één ketenpartner bevat dan geldt een verhoogd risico. Hierbij wordt onderscheid gemaakt tussen het verwerken van basispersoonsgegevens en bijzondere persoonsgegevens:

- **Bij verwerking van basispersoonsgegevens is de PIA-waarde 'Midden'.**
- **Bij verwerking van bijzondere persoonsgegevens is de PIA-waarde 'Hoog'.**

Meerdere ketenpartners per proces wijst op een brede verspreiding van gegevens buiten de organisatie en/of betrokkenheid van meerdere externe partijen bij het verzamelen en verwerken van persoonsgegevens. Beide oorzaken leiden tot een verhoogd risico op het gebied van privacy. Naast het aantal ketenpartners is ook het feit dat er een verwerkingsovereenkomst is gesloten met een externe partij een indicator voor de betrokkenheid van meerdere externe partijen bij het verzamelen en/of verwerken van gegevens. Over het al dan niet aanwezig zijn van een verwerkingsovereenkomst kan op modelniveau echter niets gezegd worden.

4.4 Als in een proces de bijzondere persoonsgegevens Gezondheid, Strafrechtelijke veroordelingen of strafbare feiten of Gegevens m.b.t. kinderen worden verwerkt is de PIA-waarde 'Hoog'.

Deze regel dekt deels het verhoogde risico voor de factor 'Het verwerken van gegevens van kwetsbare personen'. In principe geldt dat voor alle persoonsgegevensverwerkende processen de zaakbetrokkene een kwetsbaar persoon kan zijn. Dit is op procesniveau dus moeilijk te onderscheiden. De redactie is er hier vanuit gegaan dat processen met bovenstaande bijzondere persoonsgegevens een grotere kans hebben om dergelijke gegevens te bevatten. Daarom zijn deze processen op Hoog gezet.

4.5 Als in een proces sprake is van doorgifte van persoonsgegevens naar het buitenland is de PIA-waarde 'Hoog'.

Met deze regel wordt het verhoogde risico van betrokkenheid van partijen van buiten de Europese Economische Ruimte (EER) afgedekt.

Dit is de enige regel waarbij ook bij verwerking van niet-bijzondere persoonsgegevens de PIA-waarde op 'Hoog' gezet is.

Wanneer er sprake is van doorgifte van persoonsgegevens naar het buitenland staat in het model-DSP het veld *Doorgifte buitenland* op het tabblad AVG op *Ja*.

4.6 Onderzoeks- en archiveringsprocessen waarin persoonsgegevens worden verwerkt leiden tot een verhoogd risico. Hierbij wordt onderscheid gemaakt tussen het verwerken van basispersoonsgegevens en bijzondere persoonsgegevens:

- **Bij verwerking van basispersoonsgegevens is de PIA-waarde 'Midden'.**
- **Bij verwerking van bijzondere persoonsgegevens is de PIA-waarde 'Hoog'.**

Voor deze processen geldt een verhoogd risico omdat er sprake kan zijn van koppeling, vergelijking of verrijking van persoonsgegevens uit verschillende bronnen.

4.7 Wanneer registraties basispersoonsgegevens bevatten is de PIA-waarde 'Midden'.

4.8 Wanneer registraties bijzondere persoonsgegevens bevatten is de PIA-waarde 'Hoog'.

Verwerking van gegevens die betrekking hebben op gehele of grote delen van de bevolking leidt tot een verhoogd risico. Het gaat hier om grote hoeveelheden persoonsgegevens, die bevinden zich over het algemeen in registraties. Vandaar de regel dat registraties met persoonsgegevens leiden tot een verhoogd risico.

4.9 Als in een proces wettelijk voorgeschreven persoonsnummers (bijv. BSN) worden verwerkt is de PIA-waarde 'Midden'.

Het verwerken van het BSN heeft geen risico verhogend effect en valt daarmee onder het basisniveau voor alles waar persoonsgegevens in worden verwerkt.

4.10 Als een proces niet onder één van bovenstaande regels valt, krijgt het de PIA-waarde 'Laag'.

Niet in het Model-DSP meegenomen factoren

De volgende factoren leiden ook tot een verhoogd privacyrisico, maar zijn niet toe te passen op modelniveau:

- *Betrokkenheid van meerdere interne partijen bij het verzamelen en verwerken van gegevens*
  In het model-DSP wordt de organisatie als één geheel beschouwd en dus is het hogere risico niet aan te geven. Een indicator zou kunnen zijn dat er meerdere proceseigenaren zijn, maar daar is op modelniveau niets over te zeggen.

- *Brede verspreiding van gegevens binnen de organisatie*
  In het model-DSP wordt de organisatie als één geheel beschouwd en dus is het hogere risico niet aan te geven.

- *Grote impact van het intrekken van toestemming voor de verwerking van persoonsgegevens voor betrokkene*
  Dit zullen vooral processen zijn waarin ook bijzondere persoonsgegevens worden verwerkt, voor deze processen staat het risico al op 'Hoog'.

- *Doorgave van gegevens aan andere partijen die niet in lijn der verwachting van betrokkene is*
  De organisatie is verplicht om de betrokkene te informeren over wat er met zijn/haar persoonsgegevens gebeurt. Dit wordt daarom als een algemeen risico gezien dat niet specifiek op één proces toepasbaar is. Het is daarom niet toepasbaar in het Model-DSP.

- *Onduidelijkheid bij betrokkene over verwerking*
  De organisatie is verplicht om de betrokkene te informeren over wat er met zijn/haar persoonsgegevens gebeurt. Dit wordt daarom als een algemeen risico gezien dat niet specifiek op één proces toepasbaar is. Het is daarom niet toepasbaar in het Model-DSP.

- *Geen mogelijkheid tot inzien/wijzigen/verwijderen van gegevens door betrokkene*
  Dit is een organisatiespecifieke factor en daarom niet toepasbaar in het Model-DSP.

- *Gebruik van nieuwe technologie (bijv. intelligente transportsystemen, locatie of volgsystemen op basis van GPS, mobiele technologie of gezichtsherkenning) of technologie die bij het publiek vragen of weerstand op kan roepen (bijv. biometrie, RFID of behavioural targeting).*
  Gebruikte technologie is verschillend per organisatie en daarom niet toepasbaar op het model-DSP.

- *Onduidelijkheid over de verantwoordelijke voor de verwerking van persoonsgegevens*
  Aangezien de organisatie zelf verantwoordelijk is voor het bepalen van de verantwoordelijke, wordt dit niet meegenomen in het Model-DSP.

- *Niet gewaarborgde kwaliteit van gegevens*
  Dit wordt in het model-DSP weergegeven door middel van de BIA-classificatie op Integriteit.

- *Beslissingen over betrokkene op basis van gegevens die geen volledig en actueel beeld van betrokkene geven*
  Dit wordt in het model-DSP weergegeven door middel van de BIA-classificatie op Integriteit.

- *Opstelling van profielen die tot uitsluiting of stigmatisering kunnen leiden*

  Het model-DSP bevat geen werkprocessen die uitgaan van profilering.

- *Geen vastgestelde bewaartermijn*
  Aan alle model-DSP-werkprocessen hangen resultaattypen met een geldige waardering.

- *Geen vernietiging van gegevens na afloop bewaartermijn*
  Dit is een organisatiespecifieke factor en die betrekking heeft op de informatiesystemen of de archiefbestanden die lokaal aan de zaaktypen en registraties worden gekoppeld. Dit punt is daarmee niet toepasbaar in het model-DSP.

4.6 Duurzame toegankelijkheid

Bij duurzame toegankelijkheid gaat het om de vraag of informatie die gedurende lange(re) tijd beschikbaar moet blijven, bijvoorbeeld vanwege de historische waarde, dusdanig wordt beheerd en bewaard dat deze ook na lange tijd nog vindbaar, raadpleegbaar en interpreteerbaar is. Als basis voor de uitvoering wordt gebruik gemaakt van de selectielijsten die voor de verschillende sectoren zijn opgesteld (bijv. de selectielijst gemeenten en intergemeentelijke organen 2020).

De eis om zo'n risicoanalyse uit te voeren is opgenomen in de Handreiking KIDO. KIDO geeft echter niet aan welke risicoklassen hierbij moeten worden onderscheiden. In lijn van de gebruikte risicoklassen voor informatiebeveiliging en privacy hanteren we in het model-DSP de risicoklassen Laag, Midden en Hoog:

- **Laag**: het standaard beheerregime voor informatiebeheer is afdoende. Dit garandeert dat informatie voor ten minste 10 jaar toegankelijk (vindbaar, raadpleegbaar en interpreteerbaar) is.
- **Midden**: het beheerregime moet garanderen dat de informatie minimaal 40 jaar toegankelijk (vindbaar, raadpleegbaar en interpreteerbaar) is.
- **Hoog**: het beheerregime moet garanderen dat de informatie meer dan 40 jaar toegankelijk (vindbaar, raadpleegbaar en interpreteerbaar) is.

In het model-DSP zijn *bewaartermijnen* gekoppeld aan resultaattypen. Een proces kan meerdere resultaattypen hebben en per resultaattype is een bewaartermijn aangegeven die is afgeleid uit de selectielijst voor de betreffende sector. Ook is aangegeven wat het startmoment is van de bewaartermijn. Hierbij zijn verschillende opties: het moment van afhandeling van de zaak (het proces), het moment van het beëindigen van een overeenkomst, etc. De periode van het starten van de zaak tot het bereiken van het startmoment van de bewaartermijn wordt in selectielijsten de *procestermijn* genoemd. In de hieronder beschreven regels wordt gesproken over de *bewaarperiode*. Dit is de door de model-DSP-redactie ingeschatte periode vanaf het begin van de zaak tot het eind van de bewaartermijn (de maximale procesperiode + de bewaartermijn), voor het 'standaardresultaattype'. Het standaardresultaattype is het resultaattype dat hoort bij het 'normale' procesverloop.

Regels

De volgende regels zijn gehanteerd om de risico's voor duurzame toegankelijkheid van processen te bepalen:

5.1 Als het proces een resultaattype heeft met waardering 'blijvend te bewaren' is de risicoclassificatie duurzame toegankelijkheid 'Hoog';

Blijvend te bewaren dossiers bevatten informatie die voor het nageslacht bewaard moet worden en dus moet de toegankelijkheid op lange termijn worden gewaarborgd.

5.2 Als de bewaarperiode van een proces langer is dan 40 jaar is de risicoclassificatie duurzame toegankelijkheid ‘Hoog’;

Gezien de snelheid van de technologische ontwikkelingen is het verstandig om informatie die langer dan 40 jaar toegankelijk moet worden gehouden onder hetzelfde beheerregime te plaatsen als blijvend te bewaren informatie.

5.3 Als de bewaarperiode van een proces langer is dan 10 jaar maar minder dan 40 jaar is de risicoclassificatie duurzame toegankelijkheid ‘Midden’;

De grens van 10 jaar is hier gekozen omdat bij standaardprocessen de bewaarperiode typisch 10 jaar of minder is. Wanneer de bewaarperiode groter is dan dat is er derhalve een specifiek belang waardoor langere toegankelijkheid gewaarborgd moet worden.

5.4 In alle andere gevallen is de risicoclassificatie duurzame toegankelijkheid ‘Laag';