Whitepaper

Het model-DSP als rubriceringsschema

Versie 1.5, 1 augustus 2019

vhic bron van vernieuwing

De BIO en informatieveiligheid en privacybescherming in de overheid

Informatieveiligheid en bescherming van persoonsgegevens zijn belangrijke aspecten 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. Daarnaast geldt voor alle organisaties de Algemene Verordening Gegevensbescherming (AVG) die regelt hoe moet worden omgegaan met persoonsgegevens. Zowel de BIO als de AVG schrijven voor dat een organisatie risicoanalyses uitvoert met betrekking tot informatieveiligheid (de BIA's) en privacy (de PIA's).
In de model-DSP's voor gemeenten, waterschappen 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 dit whitepaper wordt toegelicht hoe de redactie dit heeft aangepakt en er wordt een verantwoording gegeven voor de hierbij gemaakte keuzes.

Gehanteerde terminologie

We sluiten in dit whitepaper waar mogelijk aan bij de terminologie die gehanteerd wordt in BIO en AVG. 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 (Engels: DPIA, Data Protection Impact Analysis) 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) en BBN3 (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).

Rubriceringsschema
Een rubriceringsschema is een overzicht van alle informatie in de organisatie gerubriceerd (of geclassificeerd) naar gewenste beschikbaarheid, integriteit en vertrouwelijkheid. Het doel van rubricering is om te zorgen voor een passend beschermingsniveau voor alle informatie binnen een organisatie. Om tot een volwaardig rubriceringsschema te komen is het nodig 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 zo'n schema bij veel organisaties nog in de kinderschoenen.

Issues met de standaardaanpak

De 'standaardvorm' waarin een BIA of PIA 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 incidenten met betrekking tot vertrouwelijkheid, integriteit, beschikbaarheid en privacy. Om tot een compleet rubriceringsschema te komen is het nodig om voor *alle* processen en systemen BIA's en PIA's uit te voeren. Of in ieder geval voor die 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 en deze komen alleen al om die reden in aanmerking voor een BIA en PIA.
Omdat het natuurlijk 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 je 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 kunnen 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, te meer daar er in de BIO gewerkt wordt met de algemene categorieën Laag, Midden en Hoog. Dit zijn moeilijk operationaliseerbare begrippen. De BIO doet weliswaar een poging tot nadere duiding van deze categorieën maar het vergt enige ervaring om deze 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 compleet en consistent rubriceringsschema te komen.

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 met 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 rubriceringsschema voor de BIO.
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, voor waterschappen en voor onderwijsinstellingen). Deze model-DSP's worden onderhouden door een centrale redactie en worden geleverd met tooling (de i-Navigator) waarmee het model getuned kan worden naar de eigen organisatie.

Het model-DSP als rubriceringsschema

Processen en registraties

In de voorafgaande paragrafen is duidelijk gemaakt dat het zelf ontwikkelen van een compleet rubriceringsschema 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-rubriceringsschema’ toe te voegen aan het model-DSP. Hiertoe 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)
- Basisbeveiligingsniveau (waarden 1 [Laag], 2 [Midden], 3 [Hoog])

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.

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 afgeleid uit de volgende bronnen:

- *Handreiking dataclassificatie*, IBD, versie 1.7.1, 12 april 2018
- *Baseline Informatiebeveiliging Overheid* (BIO), bijlage 2 Basisbeveiligingsniveaus, versie 1.0, 1 juni 2018
- *Privacy Impact Assessment (PIA) introductie, handreiking en* vragenlijst, Norea, versie 1.2, november 2015
- *Vragenlijst PIA*, IBD, versie 1.0, april 2014

Vervolgens zijn de regels 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 ‘Als in een proces bijzondere persoonsgegevens verwerkt worden is het vertrouwelijkheidsniveau Midden’ kan direct worden afgeleid uit de AVG metadata die al onderdeel vormen van het model-DSP.

Vervolgens zijn deze regels toegepast op alle processen in de model-DSP’s om de BIV en privacy classificaties vast te stellen. Deze zijn vervolgens vertaald naar BBN waarderingen op basis van de richtlijnen hiervoor uit bijlage 2 van de BIO.

De laatste stap was het classificeren van de model-DSP registraties. Hiertoe 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.

Conclusie

Door de gehanteerde werkwijze is een consistent en compleet model-rubriceringsschema 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 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 het rubriceringsschema 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 en de Privacy Baseline.
Uiteraard valt of staat de kwaliteit van het model- rubriceringsschema met de kwaliteit van de toegepaste regels. Daarom zijn bij wijze van verantwoording deze regels toegelicht in de volgende sectie.

Verantwoording

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

1. Beschikbaarheid

Met beschikbaarheid wordt aangegeven in hoeverre data of een informatiesysteem voor de gebruiker toegankelijk moet zijn en gebruikt kan 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. Aan de waarden is de volgende betekenis gegeven:

- Laag: Het informatiesysteem mag incidenteel uitvallen voor maximaal twee weken (ook in piekperiodes) en dit heeft nauwelijks of geen gevolgen voor burgers/gebruikers.
- Midden: Het informatiesysteem mag beperkt korte tijd uitvallen voor maximaal één week (ook in piekperiodes) en dit heeft voelbare gevolgen voor burgers/gebruikers.
- Hoog: 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

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:

- 1.2.1 Processen waar uit de naam of de omschrijving van het proces blijkt dat het een spoedeisend proces is.

- 1.2.2 Processen waarvan de binnenkomende meldingen direct door de organisatie moeten worden opgepakt.
- 1.2.3 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 bij een proces het niet beschikbaar zijn van de informatieobjecten/dossiers/resultaten 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. In het model-DSP vallen in elk geval de volgende processen onder deze categorie:

- Opstellen rampenplan
- De vergunningsprocessen die hangen aan de registratie Milieu-inrichting of het register Risicosituaties gevaarlijke stoffen
- Vergunningen / meldingen m.b.t. vuurwerk
- Evenementenvergunning/melding
- Demonstratiemelding
- Opstelling uitwijkplan
- Continuïteitsplan
- Agressie tegen personeelslid
- Arbo-incident
- Waterstand monitoring

1.5 Als een intern proces de uitvoering van één of meerdere primaire processen 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 in een proces kan leiden tot het niet behalen van wettelijke afdoeningstermijnen en daarmee tot juridische 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'.

Integriteit

Met integriteit wordt aangegeven in hoeverre informatie overeenkomt met de werkelijkheid en dat niets ten onrechte is achtergehouden of verdwenen. Hierbij gaat het specifiek om de juistheid, de volledigheid en de tijdigheid van informatie.

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.

- Laag: 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
- Midden: 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: Passende maatregelen om de juistheid, tijdigheid en volledigheid van informatie te waarborgen zijn van cruciaal belang. Het verlies van integriteit kan leiden tot zeer grote schade.

Regels

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

2.1 Als in een proces financiële transacties plaats vinden is het Integriteitsniveau ‘Hoog’.
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.

2.2 Als een proces tot een besluit of beschikking leidt met een financiële transactie (m.u.v. leges) tot gevolg is het Integriteitsniveau ‘Hoog’.
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.

2.3 Als een proces leidt tot een besluit of beschikking met moeilijk te herstellen gevolgen is het Integriteitsniveau ‘Hoog’.
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. Voor besluiten met moeilijk te herstellen gevolgen is het dus des te meer van belang dat deze besluiten op basis van integere informatie genomen worden. 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 moeilijk te herstellen gevolgen.

2.4 Als een proces tot een besluit of beschikking leidt en niet onder bovengenoemde integriteitsregels valt is het Integriteitsniveau ‘Midden’.

Wanneer er in een organisatie besluiten of beschikkingen worden genomen is het hoe dan ook van belang om over integere informatie te beschikken. Het niet voorhanden hebben van integere informatie kan leiden tot verkeerde besluiten. Daarom is voor alle processen waarin besluiten of beschikkingen worden genomen de waarde voor integriteit vastgesteld op 'Midden'. Concreet gaat het hier in het model-DSP om alle processen met een documenttype *Besluit* of *Beschikking* die nog geen classificatie hebben o.b.v. bovenstaande regels.

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 In alle andere gevallen is het Integriteitsniveau 'Laag'.
Wanneer geen van bovenstaande regels van toepassing is op het proces, dan is het integriteitsniveau van het proces laag.

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. De gebruikte niveaus van vertrouwelijkheid zijn:

- Laag: Organisatievertrouwelijk - Kennisname van informatie door niet-geautoriseerden (buitenstaanders) is niet gewenst, maar leidt niet tot schade van enige omvang.
- Midden: 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: Behandelaarvertrouwelijk - Verlies van informatie heeft een grote impact, waarvan niet uit te leggen is als deze niet gerubriceerd is en beschermd wordt.

Regels

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

3.1 Als in een proces bijzondere persoonsgegevens verwerkt worden is het Vertrouwelijkheidsniveau 'Midden'.
Bijzondere persoonsgegevens 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). Hier geldt dat alle persoonsgegevens behalve *Basispersoonsgegevens* onder bijzondere persoonsgegevens[1] vallen.

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

[1] Bijzondere persoonsgegevens wordt hier opgevat als bijzondere persoonsgegevens zoals bedoeld in de AVG, alsmede persoonsgegevens met betrekking tot kwetsbare groepen (waaronder kinderen) en financiële persoonsgegevens.

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.

3.3 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 terecht komt, 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*.

3.4 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*.

3.5 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*, *Inkoop*, *Contract* of *Uitgifte*[2] hier onder.

3.6 Als een proces vertrouwelijke informatie bevat die kan leiden tot aansprakelijkheidsstelling op basis van wettelijke of contractuele verplichtingen is het Vertrouwelijkheidsniveau 'Midden'.
Wanneer bekendwording van vertrouwelijke informatie leidt tot een aansprakelijkheidsstelling 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.

3.7 Als er contractuele of wettelijke verplichtingen zijn die Vertrouwelijkheid Midden/Hoog vereisen dan Vertrouwelijkheid Midden/Hoog.
Processen waarin (persoons)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'.

3.8 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

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

vallen ook onder deze regel. In het model-DSP voor Onderwijs vallen hier tevens de processen met vertrouwelijke informatie over studenten onder.

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

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

3.10 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
- Processen omtrent het benoemen, en ontslaan van bestuurders (burgemeester, dijkgraaf, 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

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

En in het DSP voor Waterschappen tevens voor:

- Proces verbaal opstelling
- Boeterapport
- Handhaving Bestuursdwang
- Handhaving Last onder dwangsom

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.

Basisbeveiligingsniveau

De BIO heeft drie Basisbeveiligingsniveaus (BBN) vastgesteld 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 basisbeveiligingsniveau's 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.
- BBN3: Bescherming van informatie met de rubricering Departementaal Vertrouwelijk of vergelijkbaar, waarbij weerstand tegen statelijke actoren of vergelijkbare bedreigers 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.

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

- Wanneer Beschikbaarheid, Integriteit en Vertrouwelijkheid Laag zijn geldt BBN1
- In alle andere gevallen geldt BBN2
- BBN3 wordt vooralsnog niet toegekend in het model-DSP, aangezien dit niveau nog in ontwikkeling is.

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.

Toegepaste regels en operationalisatie

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

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.

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.

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.

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.

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 persoonsgegevens-verwerkende 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.

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* (tabblad AVG in de i-Navigator) op *Ja*.

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.

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

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.