SAMENWERKINGSVERBAND
AMSTELLAND EN DE
MEERLANDEN

IBP-beleid

VO Samenwerkingsverband Amstelland en de Meerlanden

laatst bijgewerkt: 28-06-2018

opgesteld door de interne werkgroep IBP:
Brenda Martin
Joanne Boeschoten
Jolanda van Veen
Frans Jordaan

bestuurlijks vastgesteld op: 17-07-2018

1 Inleiding

Het VO Samenwerkingsverband Amstelland en de Meerlanden (SWVAM) voert taken uit in het kader van de wetgeving Passend Onderwijs, die zijn beschreven en vastgelegd in het meerjaren Ondersteuningsplan (http://swvam.nl/wp-content/uploads/2017/12/Ondersteuningsplan-2018-2022-SWV-Amstelland-en-de-Meerlanden.pdf). Het SWVAM kan deze taken alleen uitvoeren op basis van persoonsgegevens van de leerlingen die het betreft. Deze gegevens worden door ons verwerkt met software, apparatuur en andere middelen.
Tevens is SWVAM werk- en opdrachtgever en beschikt het vanuit deze hoedanigheid over persoonsgegevens van haar medewerkers.

Vanwege het werken met persoonsgegevens is het SWVAM gehouden aan de Algemene Verordening Gegevensbescherming (AVG). Daartoe dient het SWVAM beleid te formuleren voor Informatiebeveiliging en Privacy (IBP). In dit document beschrijven wij ons IBP-beleid. We gaan in op de uitgangspunten en indicatoren en werken uit welke maatregelen we nemen om aan de eisen van de AVG te voldoen. De basisopzet van dit document is ontleend aan Kennisnet.

Waarom is IBP-beleid van belang?
Het uitwisselen en verwerken van persoonsgegevens en de middelen waarmee dit gebeurt, worden blootgesteld aan een groot aantal, al dan niet opzettelijke, bedreigingen en risico's. Het kan variëren van een gerichte aanval om gegevens te stelen, of systemen te ontregelen tot een vergissing van een medewerker of een situatie van overmacht. Wanneer dit optreedt kunnen persoonsgegevens kwijtraken en in handen van onbevoegden komen. Als dat gebeurt is er sprake van een beveiligingsincident, dat kan leiden tot een datalek. Dit is een inbreuk is op de privacy van degenen op wie de persoonsgegevens betrekking hebben, verder te noemen: de betrokkenen.
Naarmate een organisatie meer middelen gebruikt in de uitwisseling en verwerking van persoonsgegeven, wordt de noodzaak om doeltreffende preventieve en reactieve maatregelen te nemen, deze actueel te houden en regelmatig te evalueren, groter. Dit geldt ook voor SWVAM.

Waar richt IBP-beleid zich op?

Informatiebeveiliging is het doorlopende proces voor het beschermen van SWVAM tegen het risico op het ontstaan van een datalek. Het richt zich op drie aspecten:

- Beschikbaarheid; informatie en aanverwante bedrijfsmiddelen zijn toegankelijk wanneer nodig;
- Integriteit; informatie en verwerkingsmethoden bevatten zo min mogelijk fouten;
- Vertrouwelijkheid; informatie is alleen toegankelijk voor diegenen die daartoe bevoegd zijn.

Privacy gaat om de bescherming van persoonsgegevens conform de huidige wet- en regelgeving. Hierin is onder meer geregeld op welke manier instemming gegeven wordt, welke bewaartermijnen er gelden en hoe er met de betrokken gecommuniceerd dient te worden. Door het goed toepassen van informatiebeveiliging kan aan deze wetgeving worden voldaan. Informatiebeveiliging is daarom een integraal onderdeel van privacybeleid. Voor de bescherming van de persoonsgegevens van leerlingen beschikt SWVAM over een privacyreglement, dat bestuurlijk is vastgesteld op 11-02-2016 (http://swvam.nl/wp-content/uploads/2013/11/Privacyreglement_SWV_VO-Amstelland-en-de-Meerlanden-vastgesteld-11022016.pdf)

2 Doel en reikwijdte

Het IBP-beleid heeft als doelen:

- Het waarborgen van de continuïteit in de casussen waar het SWVAM bij betrokken is[1];
- Het waarborgen van de privacy van betrokkenen, waardoor beveiligingsincidenten en de eventuele gevolgen hiervan worden voorkomen of tot een minimum beperkt blijven.
- Duidelijk maken waar de verantwoordelijkheden rondom informatiebeveiliging en privacy zijn belegd.

Het IBP-beleid is een leidraad voor alle medewerkers binnen SWVAM, die in aanraking komen met persoonsgegevens. Er is geen onderscheid tussen medewerkers 'in dienst van', 'gedetacheerd bij' of 'ingehuurd door' SWVAM. Het is van toepassing op:

- de fysieke locatie van SWVAM;
- de technische middelen die door de medewerkers gebruikt worden, zoals vaste computers, latops, tablets en mobiele telefoons;
- de digitale opslag van persoonsgegevens binnen de netwerkomgeving en op losse gegevensdragers;
- de papieren opslag van persoonsgegevens
- het mondeling delen van persoonsgegevens.

Het IBP-beleid maakt voor leerlingen, ouders, medewerkers en andere betrokkenen inzichtelijk op welke wijze er met hun persoonsgegevens omgegaan wordt. Dit beleidsdocument is via onze website open toegankelijk. Onderdeel van het IBP-beleid is een aantal protocollen dat het SWVAM volgt, zoals het eerder genoemde prvacyreglement, de procedure voor het omgaan met datalekken en het reglement voor de functionaris gegevensbescherming.

3 Uitgangspunten

De belangrijkste uitgangspunten voor ons IBP-beleid:

- Ons IBP-beleid dient te voldoen aan alle relevante wet- en regelgeving; met name genoemd is de Algemene Verordening Gegevensbescherming (AVG), die in mei 2018 in gaat (zie verder paragraaf 4);
- In het kader van de AVG is het SWVAM een 'verwerkingsverantwoordelijke'. Dit houdt in dat wij een eigen verantwoordelijkheid hebben voor het verwerken van de persoonsgegevens over leerlingen, medewerkers en andere betrokkenen die ons ter beschikking gesteld zijn. [2]
- De technische maatregelen die genomen worden om persoonsgegevens te beschemen zijn altijd up to date en voldoen aan de algemeen geldende en breed geaccepteerde beveiligingsnormen; we laten ons hierbij leiden door de richtlijnen van de Autoriteit Persoonsgegevens, de tools die Kennisnet voor het onderwijs en de samenwerkingsverbanden ontwikkelt en de deskundigheid van onze ICT-dienstverleners;
- Het SWVAM maakt met alle partijen waarmee persoonsgegevens worden uitgewisseld concrete afspraken over informatiebeveiliging en privacy (Wat is de grondslag van de uitwisseling? Welke gegevens wisselen we uit? Hoe vindt de wisseling plaats? Voor welke onderdelen is uitdrukkelijke toestemming van de betrokkenen nodig? Hoe verkrijgen we deze toestemming?[3]);

---

[1] Bijv. bij het kwijtraken van papieren en/of het wegvallen van medewerkers.

[2] Wettelijk gezien kan er geen sprake zijn van 'eigenaarschap' over deze gegevens, omdat het in hoofdzaak digitaal aangeleverde informatie betreft.

[3] Wij werken alleen met actieve toestemming. Stilzwijgend toestemming verkrijgen (opt-out) gaat tegen de AVG in en wordt door ons derhalve niet geaccepteerd.

- Met partijen die in opdracht van SWVAM persoonsgegevens verwerken (de 'verwerkers')', zoals leveranciers van ICT-dienten en personeelsadministratie, worden verwerkersovereenkomsten gesloten.[4]
- Van al onze medewerkers verwachten wij dat zij binnen onze werkprocessen afspraken maken over de uitwisseling van persoonsgegevens die passen binnen de kaders van de wetgeving;
- IBP is een continu proces, dat wij jaarlijks evalueren op basis van een PDCA-cyclus;
- Binnen SWVAM gedragen gedragen wij ons verantwoordelijk ten aanzien van het veilig en betrouwbaar omgaan met persoonsgegevens die ons ter beschikking zijn gesteld; ons handelen met en communiceren over persoonsgevens is conform de vijf vuistregels van IBP:

1. **Doelbepaling en doelbinding**:
   a. leerlingen
   Wij verwerken persoonsgegevens van leerlingen alleen om ervoor te kunnen zorgen dat de leerling binnen het voortgezet onderwijs extra ondersteuning krijgt en/of op een zo passend mogelijke onderwijsplek terecht komt.

   Voor een uitgebreide beschrijving van doelbepaling en doelbinding, wordt verwezen naar het Privacyreglement van SWVAM (op 11-02-2016 vastgesteld door het Algemeen Bestuur).

   b. personeel
   Wij verwerken de persoonsgegevens van medewerkers alleen ten behoeve van de personeelsadministratie. Daaronder vallen de salarisadministratie, de facturering van dienstverlening, het verzuim- en vervangingsbeleid en de functioneringscyclus.

2. **Grondslag**
   a. leerlingen
   Het SWVAM voert taken uit in het kader van de wetgeving Passend Onderwijs, als onderdeel van de Wet op het Voortgezet Onderwijs en de Wet op het Primair Onderwijs. In de wet is vastgelegd dat een samenwerkingtsverband besluiten neemt over de toelaatbaarheid van leerlingen tot het Voortgezet Speciaal Onderwijs en het Praktijkonderwijs. Tevens is vastgelegd dat het een samenwerkingsverband aan scholen en schoolbesturen middelen kan toewijzen voor leerlingen met een extra ondersteuningsbehoefte. Om deze taken te kunnen uitvoeren heeft het SWVAM de persoonsgegevens van de betreffende leerlingen nodig.
   Voor de wijze van uitvioering van de wettelijke taken zijn regionale afspraken gemaakt met en tussen de aangesloten schoolbesturen. Deze zijn beschreven en vastgelegd in het meerjaren Ondersteuningsplan (http://swvam.nl/wp-content/uploads/2017/12/Ondersteuningsplan-2018-2022-SWV-Amstelland-en-de-Meerlanden.pdf).
   Voor een uitgebreide beschrijving van de grondslag, wordt verwezen naar het Privacyreglement van SWVAM (op 10-12-2015 vastgesteld door het Algemeen Bestuur).

   b. personeel
   Het SWVAM is werk- en opdrachtgever en voert vanuit die hoedanigheid een personeelsadministratie voor alle medewerkers die in dienst zijn, gedetacheerd zijn of ingehuurd worden.

3. **Dataminimalisatie**
   a. leerlingen

[4] tussen verschillende 'verantwoordelijken', zoals het SWVAM en de schoolbesturen, hoeven geen verwerkersovereenkomsten gesloten te worden. In de wet is al geregeld dat scholen en SWVAM persoonsgegevens mogen uitwisselen, mits dit voldoet aan de vijf vuistregels

Het SWVAM verwerkt niet meer persoonsgegevens dan strikt genomen noodzakelijk is voor de uitvoering van haar taken. Dit wordt geborgd door:

- duidelijke afspraken over werkprocessen binnen het Regioloket
- duidelijke afspraken over uitwisseling van persoonsgegevens met scholen en andere externe partners;
- de inrichting van de ICT-systemen, met name TOP-dossier.

Het SWVAM bewaart persoonsgegevens niet langer dan strikt genomen noodzakelijk is. Het bijhouden van bewaartermijnen en het verwijderen van persoonsgegevens van leerlingen is automatisch geregeld via TOP-dossier. Hierbij worden de wettelijke termijnen gehanteerd.

b. personeel

Het SWVAM verwerkt alleen persoonsgegevens van medewerkers die van belang zijn voor uitbetalen van salarissen, het voldoen van facturen, het voeren van verzuim- en vervangingsbeleid en de functioneringscyclus. Wij besteden deze werkzaamheden grotendeels uit aan Dyade en het Risicofonds. Met deze partijen worden verwerkersovereenkomsten gesloten.

4. **Transparantie**

Het SWVAM zorgt ervoor dat betrokkenen tijdig en voldoende geïnformeerd zijn over de wijzewaarop hun persoonsgegevens gebruikt en bewaard worden. Deze informatievoorziening vindt ongevraagd plaats. Het IBP-beleid en het privacyreglement zijn vrij toegankelijk via de website.

Recht op inzage

Alle betrokkenen hebben recht op inzage in de persoonsgegevens die SWVAM van hen verwerkt.

a. leerlingen

Voor de verwerking van persoonsgegevens van leerlingen gebruiken wij in principe TOP-dossier. In de fase van implementatie gebruiken wij nog enige tijd ons Citrix-platform, naast TOP-dossier. Op termijn zullen persoonsgegevens van leerlingen nog sporadisch buiten TOP-dossier verwerkt worden.

Binnen de beveiligde omgeving van TOP-dossier worden aan ouders en leerling inzages in het dossier verstuurd. Mochten ouders en leerling ook andere notities betreffende de leerling willen inzien, dan kan hiertoe een verzoek worden ingediend bij de casemanager van het Regioloket. De casemanager bespreekt het verzoek met de coördinator van het Regioloket en maakt, indien het verzoek gehonoreerd wordt, afspraken over de inzage met de aanvrager. Indien er geen casemanger (meer) is, kan het verzoek rechtstreeks worden ingediend bij de coördinator van het Regioloket.

b. personeel

Voor de verwerking van persoonsgegevens van medewerkers wordt gebruik gemaakt van de eigen adminstratie van SWVAM en van de dienstverleningen van Dyade en het Risicofonds. Voor inzage in de persoonsgegevens kan een medewerker terecht bij zijn/haar direct leidinggevende.

Het recht om vergeten te worden

Het SWVAM biedt betrokkenen, in overeenstemming met het recht om vergeten te worden (AVG art. 17), de mogelijkheid om de persoonsgegevens te verbeteren, aan te vullen, te verwijderen of af te schermen. Dit is van toepassing in de voilgende gevallen:

- als gegevens feitelijk onjuist zijn;

- als de verwerking onvolledig of ‘niet terzake dienend’ is;
- als de verwerking op een andere manier in strijd met de wet blijkt.

a. leerlingen
Een verzoek tot aanpassing of verwijdering van persoonsgegevens van een leerling kan worden ingediend bij de casemanager van het Regioloket. De casemanager bespreekt het het verzoek met de coördinator van het Regioloket en voert, indien het verzoek gehonoreerd wordt, de aanpassingen door. De aanvrager wordt hiervan op de hoogte gesteld. Indien er geen casemanger (meer) is, kan het verzoek rechtstreeks worden ingediend bij de coördinator van het Regioloket.

b. personeel
Een medewerker kan een verzoek tot verwijdering of aanpassing van persoonsgegevens indienen bij zijn/haar direct leidinggevende. Deze houdt over het verzoek ruggenspraak met de directeur-bestuurder.

5. **Data-integriteit**
Het SWVAM verwerkt alleen persoonsgegevens die juist en actueel zijn en vanuit betrouwbare bronnen worden aangeleverd.

a. leerlingen
Voor de persoonsgegevens van leerlingen is dit geborgd via het werken met TOP-dossier. Scholen, leerlingen, ouders en andere betrokkenen hebben inzage in de uitgewisselde gegevens en hebben de mogelijkheid om aanvullingen en correcties voor te stellen.

b. medewerkers
De persoonsgegevens van medewerkers worden aangeleverd door de medewerkers zelf. Gegevens uit andere bronnen, zoals adviezen van bedrijfsartsen of bedrijfsmaatschappelijk werkenden, worden ter kennisgeveing en inzage altijd naar de betreffende medewerker gestuurd.

Al deze uitgangspunten vormen tevens de indicatoren voor de periodieke interne evaluaties van het IBP-beleid en voor audits die door externen uitgevoerd gaan worden.

4 Wet- en regelgeving

SWVAM voldoet aan alle, voor de uitoefening van haar taken relevante, wet- en regelgeving, waaronder:

- Algemene Verordening Gegevensbescherming (AVG)
- Wet Bescherming Persoonsgegevens
- Wet op het Primair Onderwijs, in het bijzonder de bepalingen Passend Onderwijs
- Wet op het Voortgezet Onderwijs, in het bijzonder de bepalingen Passend Onderwijs
- Leerplichtwet
- Wet goed onderwijs en goed bestuur PO/VO
- Archiefwet
- Auteurswet
- Wetboek van Strafrecht

Hiernaast zijn de bepalingen van het convenant ‘Digitale onderwijsmiddelen en privacy’ (https://www.privacyconvenant.nl/het-convenant/) leidend bij het maken van afspraken met leveranciers.

5 Organisatie

Dit hoofdstuk beschrijft hoe wij binnen het SWVAM het IBP-beleid belegd hebben. Er wordt daarbij onderscheid gemaakt tussen drie niveaus:

- Richtinggevend (strategisch)
- Sturend (tactisch)
- Uitvoerend (operationeel)

Voor elk niveau wordt beschreven welke rollen welke verantwoordelijkheden en taken hebben en wat de documenten zijn die daarbij passen.

Richtinggevend

Directeur-bestuurder
De directeur-bestuurder is eindverantwoordelijk voor IBP en stelt het IBP-beleid en de daarbij behorende maatregelen vast. Voorafgaand worden het directieberaad en de OPR ter advisering geraadpleegd. Het IBP-beleid wordt vervolgens ter goedkeuring aan de Raad van Toezicht voorgelegd.
Het IBP-beleid valt in de meerjarenbegroting onder programma 7 (Bestuur en Organisatie). Jaarlijks wordt in het bestuursjaarverslag gerapporteerd over de realisatie en evaluatie van het IBP-beleid.

Sturend

Functionaris Gegevensbescherming
De functionaris voor gegevensbescherming (FG) houdt voor het SWVAM toezicht op de toepassing en naleving van de AVG. De wettelijke taken en bevoegdheden van de FG geven deze functionaris een onafhankelijke en, waar nodig, een beschermde positie in de organisatie.
De PO- en VO-raad hebben de taken en bevoegdheden van de FG specifiek voor de samenwerkingsverbanden omschreven in het document “Handreiking functionaris voor gegevensbescherming SWV PaO”. Wij volgen de richtlijnen uit deze handreiking om tot aanwijzing van een FG te komen en een taak-functieomschrijving op te stellen. De mogelijke scenario’s hiervoor worden met elkaar vergeleken op basis van een aantal criteria. Naar verwachting vindt de besluitvorming plaats in juni 2018.

Privacy Officer
Binnen het SWVAM is de coördinator van het Regioloket aangewezen als Privacy Officer (PO). Dit is een taakgebied, zonder wettelijke basis. De PO is verantwoordelijk voor het organiseren en garanderen van privacy binnen een organisatie. De PO is nauw betrokken bij de uitvoering van het IBP-beleid binnen SWVAM. De werkzaamheden van de PO worden bewaakt door de FG.

Als Privacy Officer heeft de coördinator de volgende hoofdtaken:

- het vastgestelde IBP- beleid vertalen naar richtlijnen, procedures, maatregelen en documenten voor de gehele organisatie, in afstemming met externe partijen;
- de medewerkers van het Regioloket aansturen op IBP;
- de uniformiteit bewaken binnen SWVAM;
- het aanspreekpunt zijn voor incidenten op het gebied van informatiebeveiliging en privacy;
- de verdere afhandeling van incidenten binnen SWVAM coördineren, in afstemming en/of samenwerking met de functionaris gegevensbescherming;
- terugkoppeling en advies over IBP geven aan de directeur-bestuurder.

Concreter geformuleerd wordt van de Privacy Officer het volgende verwacht:

- ervoor zorgen dat alle medewerkers op de hoogte zijn van het IBP-beleid en de processen en maatregelen die daaruit voortkomen;
- toezien op de naleving van het IBP-beleid door de medewerkers;
- het handelen van medewerkers rond IBP evalueren binnen werkoverleggen en functioneringsgesprekken;
- een voorbeeldfunctie hebben ten aanzien van het naleven van het IBP-beleid;
- een aanspreekpunt zijn voor IBP-aangelegenheden die betrekking hebben op de medewerkers van SWVAM;

Werkgroep IBP
De werkgroep bestaat uit verschillende medewerkers binnen het SWVAM en valt onder de verantwoordelijkheid van de manager IBP. De werkgroep IBP heeft de volgende taken:

- het up-to-date houden van het IBP-beleid van SWVAM, door:
  - het volgen van landelijk trend en ontwikkelen rond IBP;
  - het periodiek doen van een risico-analyse;
  - het laten uitvoeren van audits door externen (hierover worden afspraken gemaakt met collega Samenwerkingsverbanden;
  - het ondersteunen van de medewerkers van het SWVAM, door te zorgen voor documentatie, werkprocesbeschrijvingen, technische en softwarematige bedrijfsmiddelen e.d..
- de berichtgeving verzorgen over IBP-ontwikkelingen en maatregelen naar de andere medewerkers van SWVAM;
- de berichtgeving verzorgen over IBP-ontwikkelingen en maatregelen naar externe partijen;
- de manager IBP adviseren over en ondersteunen bij het uitvoeren van het IBP-beleid.

Uitvoerend

Security Officer
Binnen SWVAM is Parentix het technisch aanspreekpunt voor incidenten en informatiebeveiliging.

Medewerker
Alle medewerkers van SWVAM hebben een eigen IBP-verantwoordelijkheid in hun dagelijkse werkzaamheden. Het privacyreglement en de geldende afspraken over het werkproces binnen het Regioloket zijn hiervoor leidend.

Waar nodig ondersteunen wij de medewerkers bij de uitvoering van hun werkzaamheden met documentatie, werkprocesbeschrijvingen, technische en softwarematige bedrijfsmiddelen e.d.. De werkgroep IBP draagt hier zorg voor.

Wij verwachten van onze medewerkers dat zij actief handelen volgens de uitgangspunten van het IBP-beleid en deze uitgangspunten ook uitdragen naar externe partijen. Wanneer zich situaties voordoen die strijdig zijn met uitgangspunten van het IBP-beleid, wordt ervan uit gegaan dat zij in eerste instantie afgaan op hun eigen oordeel en oplossend vermogen, bij voorkeur in overleg met een directe collega.
Wanneer een situatie leidt tot een groter risico op een datalek, zullen zij dit onder de aandacht brengen van de Privacy Officer en de Functionaris Gegevensbescherming.

6 overige maatregelen

Naast het beleggen van IBP-taken en benoemen van verantwoordelijkheden, nemen wij binnen het SWVAM ook andere maatregelen om de persoonsgegevens van betrokkenen te beschermen, zoals diverse technische voorzieningen en een tweetal handelingsprotocollen.

Technische voorzieningen
Het grootste gedeelte van de persoonsgegevens die met ons gedeeld worden, zijn digitaal. We willen de uitwisseling en opslag daarvan voldoende beveiligd doen. Dit stelt eisen aan de gebruikte software en apparatuur. Wij realiseren zo optimaal mogelijke beveiliging door te werken met erkende programma's en leveranciers, zoals Citrix (leverancier Parentix), TOP-dossier (leverancier Dotcomschool), Dyade, Youforce en Risicofonds. Met deze partijen sluiten wij verwerkersovereenkomsten.
Wanneer wij vinden dat de beveiliging onvoldoende optimaal is, nemen wij aanvullende maatregelen, zoals de aanschaf van betere software en bepaalde applicaties.

Daarnaast schermen wij het gebruik van de verschillende systemen en apparaten voor onbevoegden af met wachtwoorden, schermvergrendelingen e.d.. Om de niet-digitale persoonsgegevens af te schermen, zijn onze werkruimtes afgesloten als er niemand is en bevinden papieren gegevens zich altijd in afgesloten kasten. Mondelinge uitwisseling van persoonsgegevens vindt zoveel mogelijk achter gesloten deuren plaats.

Handelingsprotocollen
Ondanks ons streven naar een zo optimaal mogelijke staat van beveiliging van persoonsgegevens, zijn we niet risico-vrij. Onze maatregelen beperken de risico's, maar sluiten grotere en kleinere incidenten nooit helemaal uit. Wanneer wij te maken krijgen met een beveiligingsincident, willen we dat echter snel boven krijgen, analyseren en er de juiste maatregelen op zetten. Hoe wij dat doen is vastgelegd in ons "protocol datalekken".

Binnen SWVAM leggen wij de verantwoordelijkheid voor het handelen grotendeels bij de medewerkers zelf. Zij zijn zich zeer bewust van hun taak om de persoonsgegevens van betrokkenen voldoende te beschremen. Niettemin is er een risico dat zij, meestal ongewild, een beveiligingsincident laten ontstaan of daar via een externe partner mee geconfronteerd worden. Om hen zoveel mogelijk richtlijnen in handen te geven voor het handelen conform de AVG, stellen wij een medewerkersinstructie op. Naar verwachting zal deze in september 2018 gereed zijn.

7 documentatieplicht

In de AVG is een verantwoordingsplicht opgenomen. Dit houdt in dat wij moeten kunnen aantonen dat alle verwerkingen aan de regels voldoen. En ook dat we de juiste organisatorische en technische maatregelen hiervoor hebt genomen. Het is dus van belang om dit goed vast te leggen en hierover te communiceren. Wij doen dat via een risico-analyse, een dataregister en een privacyverklaring.

risico-analyse
De AVG schrijft voor dat er een effectbeoordeling gedaan wordt rond de gegevensbescherming binnen het SWVAM. Dit wordt een Privacy Impact Assessment (PIA) genoemd, ofwel risico-analyse. Binnen het SWVAM bevindt de risico-analyse zich in de twee fase. De eerste vond plaats in december 2016. Nadat in de tussenliggende periode een aantal maatregelen genomen is, wordt de risico-analyse in het voorjaar van 2018 herhaald. De uitkomsten daarvan zijn in juni 2018 gereed. Vanaf dat moment wordt opnieuw beoordeeld of ons pakket aan genomen maatregelen afdoende is voor het afdekken van de risico's. Uit de risico-analyse komt een classificatie voort van de verschillende per-

soonsgegevens die wij onder ons beheer hebben. De classificatie bepaalt het niveau van de beveiligingsmaatregelen die wij nemen.

dataregister
Het bijhouden van een dataregister van verwerkingsactiviteiten is een onderdeel van de verantwoordingsplicht binnen de AVG. Wanneer de Autoriteit Persoonsgegevens daarom vraagt, dient het register getoond te worden. Er geldt een aantal voorwaarden voor het opstellen van het dataregister. Het SWVAM volgt de richtlijnen van de PO- en VO-raad. Naar verwachting is ons dataregister in juni 2018 gereed.

privacyverklaring
De AVG benoemt ook een informatieplicht, die ons voorschrijft om betrokkenen duidelijk te informeren over wat wij met hun persoonsgegevens doen. Wij volgen het advies van Kennisnet om hiervoor in elk geval een (online) privacyverklaring op te stellen. Omdat hier eisen aan verbonden zijn, gebruiken wij het model privacyverklaring van Kennisnet. Naar verwachting volgt publicatie in juni 2018 via onze website.

8 communicatie

Beleid en instrumentele maatregelen zijn niet voldoende om alle risico's te minimaliseren of zelfs uit te sluiten. In de praktijk blijken incidenten vaak door ons eigen handelen of het nalaten daarvan te ontstaan. Van onwil is daarbij zelden sprake. Eerder ontstaan beveiligingsincidenten door onachtzaamheid of doordat in de snelheid van werken de aandacht voor IBP verslapt.
Daarom houden wij bij het SWVAM de aandacht en het bewustzijn van onze medewerkers en partners scherp met actieve communicatie. Wij doen dat op verschillende manieren:

- Regelmatig sturen wij een mailing rond met belangrijke informatie over de stappen die wij in het kader van ons IBP-beleid zetten.
- Wij maken afzenders die persoonsgegevens onbeveiligd met ons delen er via een standaard reply op attent dat zij in strijd met de AVG handelen. In sommige verwijderen we de persoonsgegevens direct en geven de afzender aan hoe ze voor betere beveiliging kunnen zorgen.
- Wij publiceren instructies met uitleg over de wijze waarop versleuteling van gegevens gedaan kan worden.
- Tijdens netwerkbijeenkomsten geven wij voorlichting over de implicaties en het belang van de AVG.
- Wij voeren jaarlijks een risico-analyse uit met onze medewerkers, hetgeen voor bewustwording zorgt en voor aanvullende maatregelen, indien wenselijk.
- Via onze website zijn alle relevante documenten over ons IBP-beleid voor iedereen toegankelijk. Daarnaast zorgen wij via onze website voor dooegroepgerichte informatie over de wijze waarop wij met privacy omgaan.

9 kwaliteitscyclus

Wij passen op ons IBP-beleid een PDCA-cyclus toe. Jaarlijks voeren we één of meerdere evaluaties uit en we maken afspraken met collega-samenwerkingsverbanden om via audits te toetsen of we doen wat we beloven te doen. Het evalueren, doorlichten en bijstellen van ons IBP-beleid is een taak van de interne IBP-werkgroep. Zodra dit kan, zal deze werkgroep zich hierbij laten adviseren door de nog aan te stellen Functionaris gegevensbescherming.

De ijkpunten voor onze evaluaties en audits zijn tweeledig:

- de status van de informatiebeveiliging als geheel (beleid, organisatie, risico's), afgezet tegen nieuwe ontwikkelingen, incidenten die zich voorgedaan hebben en de aanschaf van nieuwe diensten of apparatuur;
- de effectiviteit van de genomen maatregelen, afgezet tegen de eerder in dit document genoemde uitgangspunten of indicatoren.

In het bestuursjaarverslag rapporteren wij jaarlijks over de uitkomsten van de evaluatie van ons IBP-beleid.

Tenslotte merken wij op dat wij bij de uitvoering van ons IBP-beleid streven naar een balans tussen de risico's van hetgeen we willen beschermen en de materiële en financiële investeringen die we daarvoor doen. Voor het afdekken van geringe risico's doen wij geen maximale investeringen, terwijl wij voor het afdekken van hoge risico's juist optimaal willen investeren. Daarbij houden wij altijd voor ogen dat wij voldoen aan alle eisen die de AVG aan ons stelt.