

BMC

YACHT GROUP

Informatiebeveiliging en privacy in het onderwijs

Niet meer vrijblijvend



mei 2018

Partners in verbetering

Informatiebeveiliging en privacy in het onderwijs

Niet meer vrijblijvend

Inhoudsopgave

1	Informatiebeveiliging en privacy in het onderwijs - niet meer vrijblijvend	7
2	Zorgvuldig omgaan met gegevens van leerlingen, scholieren en studenten: grip krijgen op Privacy en informatiebeveiliging ...	11
3	Concreet: de aanpak van BMC	15
	Contact	18
	Colofon	18

H1 | Informatiebeveiliging en privacy in het onderwijs – niet meer vrijblijvend

Privacy en informatiebeveiliging zijn in toenemende mate een thema in het maatschappelijk debat en in de media, mede naar aanleiding van datalekken, cybercriminaliteit en beveiligingsproblemen bij publieke organisaties. Onderwijsinstellingen zijn daarop geen uitzondering.

Met ingang van 25 mei 2018 is de Algemene Verordening Gegevensbescherming (AVG) van toepassing. Deze Europese wet geeft regels voor de omgang met persoonsgegevens. De regels gelden ook voor **onderwijsinstellingen, net zoals voor gemeenten en andere maatschappelijke organisaties zoals zorginstellingen**. Het bestuur is verantwoordelijk voor de implementatie van deze wetgeving. De rechten van **leerlingen en studenten** worden versterkt en de bevoegdheden en capaciteit van de Autoriteit Persoonsgegevens als toezichthouder worden uitgebreid. Informatiebeveiliging is een belangrijke pijler in de bescherming van privacy, naast de andere eisen die de Algemene Verordening Gegevensbescherming (AVG) stelt (zie kader). De volwassenheid van **onderwijsinstellingen** op dit gebied verschilt sterk. Sommige organisaties hebben informatieveiligheid en privacy volledig ingebed in de processen. Zij toetsen op de effectiviteit van privacymaatregelen en het management stuurt bij wanneer maatregelen niet of onvoldoende blijken te voldoen. In andere organisaties ontbreekt het vaak nog aan integraal beleid, waardoor niet gewaarborgd is dat men voldoet aan de wetten en regels.

In dit whitepaper laten we zien hoe een onderwijsinstelling grip krijgt op privacy en beveiliging van gegevens en met welke praktische stappen dit kan worden gerealiseerd.

Algemene Verordening Gegevensbescherming (AVG)

De AVG geeft aan binnen welke kaders persoonsgegevens mogen worden verwerkt en beschrijft de rol van de toezichthouder, de Autoriteit Persoonsgegevens (AP).

Onderwerpen die in uw organisatie geregeld moeten zijn om te voldoen aan de wet zijn:

- Het opstellen en onderhouden van een verwerkingenregister
- rechtmatigheid van de verwerking (grondslag)
- doelbinding
- proportionaliteit en subsidiariteit)
- bewaartermijnen
- verwerkersovereenkomsten
- melding van datalekken
- gegevensuitwisseling
- informatieveiligheid

Ten opzichte van de Wbp stelt de AVG aanvullende eisen ten aanzien van bijvoorbeeld verantwoording, documentatie, evaluatie, de beoordeling van de effecten van gegevensverwerking en de verplichte aanstelling van een functionaris gegevensbescherming. Omdat er nog geen catalogus van praktische maatregelen is om te voldoen aan de eisen rond aantoonbaarheid en evaluatie in de AVG, heeft BMC een catalogus met beheersmaatregelen ontwikkeld als basis voor een degelijke implementatie.

Privacy in het onderwijs

Een eerste stap bij de inrichting van privacy op een school is het opstellen van een register met verwerkingen van persoonsgegevens. Bij die eerste stap zijn meteen al essentiële kwesties aan de orde:

- Wie mag als FG aangesteld worden en zorg ik dat deze voldoende onafhankelijk is?
- Wanneer is er toestemming van nodig van ouders nodig en wanneer niet?
- Welke informatie mag/moet wel gestuurd worden in de overdracht tussen scholen (DOD) en wat niet?
- Hoe lang mag de school een IQ onderzoek bewaren?
- Hoe lang mag de school verzuimlijsten bewaren?
- Mogen ook nog programma's/digitale middelen gebruikt worden die niet onder het privacy covenant PO/VO-raad vallen?
- Wat mag een leerkracht wel en niet mailen?
- Hoe verhouden klassenlijsten (voor met vriendjes en vriendinnetjes spelen; NAW-gegevens) en Oudercommunicatieplatforms zich tot de principes van privacy?
- Tot welke informatie krijgt een programma ontwikkelaar toegang, wanneer hij of zij voor de school een systeem bouwt?
- Moeten beide ouders altijd dezelfde informatie krijgen? En hoe komt de school dat te weten?

Ontwikkelingen die privacy en informatiebeveiliging actueel maken

Informatiebeveiliging en privacy zijn in het onderwijs nog in ontwikkeling. Het landelijk Congres IBP, dat in oktober 2017 werd georganiseerd door de PO-Raad en de VO-Raad, was een eerste aanzet. Het onderwijs heeft zich nog slechts in beperkte mate aan standaarden gecommitteerd. Voor het Hoger Onderwijs is een normenkader beschikbaar. Voor het MBO is een vergelijkbaar document opgesteld. Voor PO en VO

is op Kennisnet een Aanpak IBP gepubliceerd. De standaarden en de aanpak verwijzen naar de internationale norm voor informatiebeveiliging ISO27001 en ISO27002. Er zijn nog geen harde eisen om daaraan te voldoen. In deze normen staat hoe bestuurders risico's kunnen beheersen en welke beveiligingsmaatregelen getroffen kunnen worden, op het gebied van beleid, organisatie, personeel, gebouwbeheer en uiteraard ook ICT.

Er zijn ontwikkelingen die de noodzaak om gegevens van **leerlingen, scholieren en studenten** en medewerkers – door het waarborgen van privacy en informatiebeveiliging – steeds gewichtiger maken:

- Elke **onderwijsinstelling** verwerkt op grote schaal persoonsgegevens. In de afgelopen jaren is de privacywetgeving stap voor stap aangescherpt met de meldplicht datalekken en boetebeleid in 2016 en in 2018 met de AVG. De verwerking van persoonsgegevens moet niet alleen voldoen aan de wettelijke kaders, maar uw organisatie moet dat ook kunnen aantonen.
- Belangrijke uitgangspunten van de AVG zijn transparantie en het afleggen van verantwoording. Dit betekent bijvoorbeeld dat het schoolbestuur ouders moet informeren over het gebruik van leerlinggegevens. Ook moet een schoolbestuur verantwoording kunnen afleggen over de keuzes zijn gemaakt, bijvoorbeeld over welke gegevens de school vastlegt over leerlingen, scholieren of studenten en met wie deze gegevens binnen en buiten de school worden gedeeld.
- De Autoriteit Persoonsgegevens (AP) krijgt met de AVG als toezichthouder meer bevoegdheden en meer personeel. Vanaf nu is een overtreding voldoende voor het geven van een boete; opzet hoeft niet aangetoond te worden. Ook gaat de AP individuele klachten behandelen en kan zij een deel van het onderzoek uitbesteden aan de Functionaris Gegevensbescherming (FG) in uw eigen organisatie. Het aanstellen van een FG is voor een onderwijsinstelling verplicht, zoals ook in de handreiking FG van de PO- en VO-Raad is weergegeven.

Daarmee krijgt de toezichthouder een veel grotere slagkracht.

- In veel onderwijsinstellingen is het delen van inlogcodes, onbeveiligd mailen van gegevens over leerlingen, scholieren en studenten aan de orde van de dag. Meer mensen dan strikt noodzakelijk hebben toegang tot leerling-scholieren- en studentgegevens. Bij het delen van gegevens met andere instanties is er onvoldoende bewustzijn en inzicht in wat wel en niet mag. Verder hebben jongeren steeds meer kennis van ICT, de eerste inbreuken op leerling-/scholier-/studentvolgssystemen waarbij cijfers zijn aangepast, zijn al tot de media doorgedrongen. Ook met andere inbreuken op beveiliging en privacy van leerling-scholieren- en studentgegevens zijn onderwijsinstellingen bijzonder kwetsbaar voor misbruik van gegevens, datalekken en handhaving door de AP en de gevolgen daarvan voor de betrokken personen en voor de reputatie van de instelling.
- Datalekken, cybercriminaliteit en andere beveiligingsincidenten komen steeds meer voor. Het is niet de vraag **of** een groot incident optreedt in uw organisatie, maar **wanneer**. Een goed geïmplementeerd beleid voor informatieveiligheid en privacy maakt de kans op een incident kleiner en zorgt ervoor dat bestuurders aan hun zorgplicht voldoen. Dat maakt het beantwoorden van vragen door toezichthouders naar aanleiding van een incident een stuk gemakkelijker.
- Steeds vaker nemen individuele betrokkenen en groepen initiatieven om ontbrekende beveiligingsmaatregelen en niet adequate toepassing van privacywetgeving aan de kaak te stellen. Maatschappelijke actoren zoals nieuwsmedia en actiegroepen maken pro-actief openbaar welke organisaties tekortschieten in de beveiliging en bewaking van privacy van alle partijen die door de AVG beschermd worden.
- Van bestuurders valt dan te verwachten dat zij de organisatie adequaat kunnen vertegen-

woordigen. Zij moeten goed op de hoogte zijn van de keuzes die de organisatie heeft gemaakt bij haar beleid en ze moeten deze keuzes professioneel kunnen uitdragen. Daarvoor moeten ze 'gevoed' worden vanuit de organisatie.

- Bij de controle van de jaarrekening maken accountants steeds meer werk van hun verplichting om over de betrouwbaarheid en continuïteit van de ICT-systemen te bevinden en te rapporteren (BW 393.4).
- Eventuele boetes van de AP vormen een materieel risico wanneer privacy en informatiebeveiliging onvoldoende zijn geregeld.

Privacy en informatieveiligheid zijn breder geworden dan alleen 'een ICT-onderwerp'. Alle medewerkers hebben er een rol in en dragen er verantwoordelijkheid voor. Bij onderwijsinstellingen was er tot nu toe vaak sprake van onbekendheid met wet- en regelgeving en gebrek aan bewustzijn en kennis om informatiebeveiliging en privacy goed te regelen. Maar momenteel vragen sectorraden er aandacht voor, mede naar aanleiding van de invoering van de AVG. Bestuurders kunnen door toezichthouders worden aangesproken wanneer zij op dit gebied geen beleid ontwikkelen. Zij dragen uiteindelijk de verantwoordelijkheid voor de beveiliging en privacy van (persoons) gegevens. Gerichtte sturing door het bestuur en het management is dan ook noodzakelijk.

Het feit dat hier juridische, technische en mensaspecten en de visie op onderwijsvernieuwing bij elkaar komen, maakt informatieveiligheid tot een complexe materie. Het ligt voor de hand dat kleinere organisaties - die over het algemeen minder specialisten in dienst hebben - hierbij eerder hulp van buiten nodig hebben dan de grote organisaties.

¹ <https://nos.nl/artikel/2177030-schiedamse-leerlingen-veranderen-proefwerkcijfers-na-hack.html>

Risico's voor onderwijsinstellingen

- Ouders en leerlingen, scholieren of studenten kunnen ernstige schade lijden bij onvoldoende informatieveiligheid, omdat het om de persoonlijke levenssfeer gaat. De vertrouwensrelatie tussen de onderwijsinstelling, leerlingen en ouders komt in het geding. Persoonlijk en financieel kan dit voor leerlingen, scholieren en studenten grote gevolgen hebben, bijvoorbeeld in de verhoudingen tussen leerlingen, scholieren en studenten ('pesten') en later bij sollicitaties. Gebrek aan vertrouwen kan ook het succes van het onderwijs ernstig dwarsbomen.
- Buitenstaanders, "hackers" kunnen onderwijsresultaten manipuleren. Dat is een aanslag op de kwaliteit en integriteit van het onderwijs. Via klachten van ouders en maatregelen van toezichthouders kan de reputatieschade die zo ontstaat, leiden tot een verminderde instroom.
- De nieuwe wet geeft de AP een krachtiger positie bij toezicht en handhaving. Een AP-"inval" of andere incidenten op het gebied van privacy of informatiebeveiliging dwarsbomen altijd de normale bedrijfsvoering. Bovendien leiden ze vaak intern en extern tot veel ophef en extra kosten.
- Bij klachten of ophef is het aan de verantwoordelijke bestuurder om toelichting te geven. Bij een onvoldoende voorbereiding op kost het veel tijd - vaak in een 'stressvolle' situatie - om zijn of haar publieke optreden goed voor te bereiden en de gevolgen van de 'slechte beurt' zoveel mogelijk te beperken. Bovendien kan de positie van de bestuurder in het geding komen.
- Er ontstaat reputatieschade en geschonden vertrouwen als gevolg van datalekken, hacken en publiciteit, of wanneer de organisatie genoemd wordt in een rapport van de AP.
- Boetes en ad hoc maatregelen naar aanleiding van incidenten en publiciteit brengen financiële schade met zich mee. Daarnaast kan reputatieschade op termijn leiden tot afname van inkomsten.
- Bij de controle van de jaarrekening kunnen problemen ontstaan, zoals door onvoldoende

aantoonbare betrouwbaarheid en continuïteit van ICT-systemen. Het is niet ondenkbeeldig dat toezichthouders daarvoor boetes geven.

Het positieve spiegelbeeld van de genoemde risico's is een goed ingerichte privacy- en informatiebeveiliging. Het vertrouwen dat de instelling zich gedraagt zoals het betaamt, zorgt voor stabiliteit en goede relaties.

H2 | Zorgvuldig omgaan met gegevens van leerlingen, scholieren en studenten: grip krijgen op Privacy en informatiebeveiliging

Wat levert de zorg voor privacy en informatieveiligheid u op?

Elke organisatie behoort aantoonbaar te voldoen aan de normen, regels en wetten voor informatiebeveiliging en privacy. De gegevens van de leerling of student zijn dan goed beschermd.

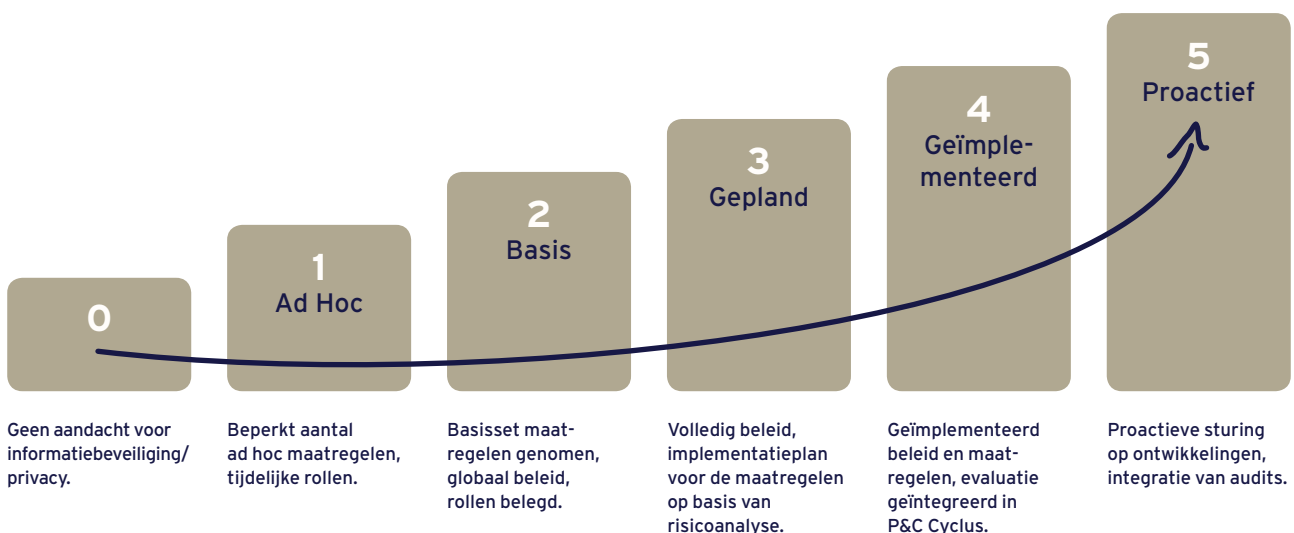
In die situatie zijn bestuurders in control. Zij kunnen bewuste, onderbouwde keuzes maken ten aanzien van risico's. Als er zich onverhoopt toch een incident voordoet, is de organisatie klaar om erop te reageren. Zij kan het lekken van informatie vaststellen, stoppen, het datalek melden bij de AP en maatregelen treffen om herhaling te voorkomen. Bovendien staan informatieveiligheid en privacy voortdurend in het licht van verbetering.

Bestuurders, management en medewerkers staan ervoor dat er passende maatregelen getroffen zijn om incidenten te voorkomen. Dat vormt ook een goede basis voor gesprekken met medezeggenschaporganen, advies- en toezichtorganen en met de samenleving als geheel, waarin privacy en

informatieveiligheid steeds vaker aan de orde komen. Zo wordt met een goed ingerichte informatieveiligheid en privacy het vertrouwen van leerlingen, studenten en hun ouders in uw organisatie versterkt.

Waar staat uw organisatie in de actuele ontwikkeling?

Het is lastig om het geheel te overzien wanneer je er midden in staat. Een blik van buiten zorgt voor onafhankelijkheid en brengt 'blinde vlekken' aan het licht. De onafhankelijke, maar deskundige buitenstaander stelt u in staat om bewuste keuzes te maken bij het treffen van maatregelen of het accepteren van risico's. Vervolgens kunt u de nodige maatregelen implementeren, al of niet met externe ondersteuning.



BMC kan u helpen: stap voor stap

De volledige invoering van een passende informatiebeveiliging volgens de voor het onderwijs opgestelde normen omvat meer dan honderd beheersmaatregelen. Dat gaat niet van de ene op de andere dag. De gestage ontwikkeling naar de gewenste status van uw organisatie kent verschillende, te onderscheiden stadia. Stapsgewijze invoering maakt het proces beheersbaar. Het ijkken van motiverende mijlpalen op weg naar volledige conformiteit zorgt voor overzicht in het voortgangsproces.

Wij onderscheiden vijf implementatieniveaus:

Implementatieniveau 0: onbekend

Er is geen aandacht voor informatieveiligheid. Deze situatie is met name aan de orde in organisaties in oprichting. Alle aandacht is gericht op het doel, de doelgroep en de medewerkers van de organisatie. "Gegevensbeveiliging? Dat zien we later wel."

Implementatieniveau 1: ad hoc

De status:

Op dit niveau ontstaan de eerste activiteiten, meestal op operationeel niveau. Rollen - zoals die van privacyofficer (ook: privacybeheerder) of securityofficer (ook: informatieveiligheidsbeheerder of CISO) - worden niet of alleen tijdelijk, bijvoorbeeld in een project, benoemd. Maatregelen worden getroffen in specifieke deelgebieden of als onderdeel van de implementatie van nieuwe systemen. Vaak ligt dan het accent op technische beveiliging. De controle vindt plaats in de marge van andere controles, zoals de controle van de jaarrekening of de certificering van het primaire proces. De resultaten kunnen aanleiding zijn om

meer aandacht aan privacy en/of informatieveiligheid te besteden, als opstap naar het volgende implementatieniveau.

De ontwikkeling:

Van ad hoc naar basis

- Voor privacy wordt een inventarisatie van verwerking van persoonsgegevens gemaakt en deze wordt getoetst aan wet- en regelgeving.
 - De uitvoering van het actieplan brengt de organisatie naar het niveau 'basis'.
 - Voor informatieveiligheid wordt een scan gemaakt op grond van een basisset van beveiligingsmaatregelen.
 - Daarop volgt een plan-van-aanpak voor de implementatie van de basisset van maatregelen.
-

Implementatieniveau 2: basis

De status:

Op het basisniveau is benoemd welke functionarissen de sleutelrollen vervullen. Zij gaan het beleid en de implementatie daarvan vorm te geven. Daarvoor worden ze opgeleid. Het beleid krijgt vorm in algemene termen en wordt gespiegeld aan wet- en regelgeving. De meest voor de hand liggende maatregelen zijn getroffen. Voor privacy is er een verwerkingsregister, de rechtmatigheid van de bewerkingen is gewaarborgd. Verwerkersovereenkomsten zijn afgesloten en processen rond de meldplicht datalekken zijn ingericht. Voor informatieveiligheid zijn er basismaatregelen op het gebied van gedrag van medewerkers, fysieke beveiliging en beveiliging van netwerken, systemen en eindgebruikersapparaten. Dat schept de uitgangssituatie om privacy en informatieveiligheid structureel op te pakken.

De ontwikkeling:

Van basis naar gepland

- Structureel oppakken bestaat uit een goede zelfevaluatie van de maatregelen die al getroffen zijn ten opzichte van de maatregelen die nodig zijn om duurzaam te voldoen aan de formele normen en aan de privacywetgeving.
- Omdat er nog geen catalogus van praktische maatregelen is om te voldoen aan de eisen rond aantoonbaarheid en evaluatie in de AVG, heeft BMC een catalogus met beheersmaatregelen ontwikkeld als basis voor een degelijke implementatie.
- Naast de zelfevaluatie wordt er voor informatieveiligheid een risicoanalyse en een dataclassificatie uitgevoerd.
- Op basis daarvan wordt voor zowel privacy als informatieveiligheid beleid verder uitgewerkt voor de deelgebieden binnen de organisatie.

Implementatieniveau 3: gepland

De status:

Op dit niveau is er integraal beleid geformuleerd dat de gehele privacywetgeving en de normen voor onderwijsinstellingen omvat. Voor informatieveiligheid zijn op basis van een risicoanalyse en het principe 'pas toe of leg uit' ('comply or explain') de te implementeren maatregelen gekozen en geprioriteerd. Deze zijn vaak nog niet volledig geïmplementeerd. Wel wordt daar in deze fase actief aan gewerkt door de maatregelen uit te werken in bijvoorbeeld procesbeschrijvingen, praktische richtlijnen en gedragscodes. Daarbij zijn steeds meer disciplines betrokken, zoals HR, facilitaire zaken, lijnmanagers en proceseigenaren in het primaire proces.

De ontwikkeling:

Van gepland naar geïmplementeerd

- Alle medewerkers worden bewust gemaakt van hun verantwoordelijkheid voor privacy en informatieveiligheid. Dit wordt bijvoorbeeld

besproken tijdens werkoverleggen.

- Door middel van geregeld voortgangsoverleg en een eventuele herhaling van de zelfevaluatie en risicoanalyse wordt de voortgang bewaakt en bijgestuurd. Daarbij is ook de hoogste leiding van de organisatie op gezette tijden betrokken.

Implementatieniveau 4: geïmplementeerd

De status:

Op dit niveau zijn het beleid en de maatregelen volledig geïmplementeerd. Ze worden eventueel bijgesteld op basis van periodieke evaluaties en risicoanalyses, volgens de 'plan-do-check-act' cyclus die ook uit het kwaliteitsmanagement bekend is. Dat maatregelen worden uitgevoerd, is aantoonbaar. Dit wordt ook bewaakt in de P&C-cyclus en getoetst door middel van interne en externe audits. Voorafgaand aan belangrijke wijzigingen in processen en systemen wordt de impact ervan onderzocht op privacy en informatieveiligheid. Op dit niveau kan ook een audit met succes worden doorlopen.

De ontwikkeling:

Van geïmplementeerd naar pro-actief

- Nu krijgt - vanuit de rust dat de actuele situatie goed verankerd is - de toekomstvisie een hogere plaats. Er wordt, naast de bewaking van alle afspraken en interne regels, ook vooruitgekeken naar verwachte en denkbare ontwikkelingen op het gebied van wet- en regelgeving en techniek. Ook worden andere actuele en toekomstige ontwikkelingen binnen de organisatie bij dit perspectief betrokken, zoals organisatieveranderingen, de invoering van nieuwe informatiesystemen, of nieuwe samenwerkingsvormen.

Implementatieniveau 5: proactief

De status:

Op dit niveau krijgt – op basis van de rust dat de actuele situatie goed verankerd is – de toekomstvisie een grotere plaats. Er wordt, naast de bewaking van alle afspraken en interne regels, ook vooruitgekeken naar verwachte en denkbare ontwikkelingen op het gebied van wet- en regelgeving en techniek. Ook worden andere actuele en toekomstige ontwikkelingen binnen de organisatie bij dit perspectief betrokken, zoals organisatieveranderingen, de invoering van nieuwe informatiesystemen, of andere samenwerkingsvormen.

Naast de uitvoering van de maatregelen is er veel aandacht voor de effectiviteit ervan. Testen van de beveiliging door externe technische specialisten (in de vorm van ‘penetratietesten’) kunnen daaraan bijdragen. Maatregelen uit verschillende normen worden gecombineerd en op elkaar afgestemd.

Op het niveau ‘proactief’ strekt de bemoeienis zich ook uit tot ketenpartners ten aanzien van privacy en informatieveiligheid. Op basis van deze implementatieniveaus geeft BMC inzicht in waar uw organisatie staat. Zowel ten aanzien van beleid als ten aanzien van de maatschappelijke beeldvorming hebben deze partners immers een aanzienlijke invloed op uw prestaties en de resultaten die u boekt voor uw cliënten.

De ontwikkeling:

BMC kan voor u onderzoeken op welk niveau uw organisatie momenteel staat en of dat voor de verschillende onderdelen van uw organisatie in gelijke mate geldt. En laat BMC u helpen uw ambities en mogelijkheden te vertalen in het stappenplan dat past bij uw school of andere onderwijsinstelling.

Uw resultaat

De begeleiding van BMC draagt in belangrijke mate bij aan het resultaat dat elke gemeente voor haar burgers, bedrijven en maatschappelijke organisaties wil realiseren: optimale betrouwbaarheid op het gebied van privacy en informatieveiligheid. Het vertrouwen dat alle gegevens bij in goede handen zijn, staat in de lokale samenleving en daarbuiten niet ter discussie. Bestuurders en medewerkers zijn zich bewust van hun verantwoordelijkheden en handelen daarnaar. Risico’s voor alle partijen – inclusief voor uw organisatie en haar bestuurders en medewerkers zelf – zijn tot een minimum beperkt. Er is ruimte om tijdig anticiperend na te denken en te handelen ten aanzien van toekomstige ontwikkelingen. Aan deze gedachtevorming kunnen bestuurders, medewerkers en medezeggenschapsorga­nisa­ties deel­nemen op basis van ruim voldoende kennis en kunde. De school of andere onderwijsorganisatie neemt in de regio, de provincie en op landelijk niveau een verantwoorde en vertrouwenwekkende plaats in in de rangorde van publieke organisaties die hun zaken goed op orde hebben ten aanzien van privacy en informatiebeveiliging.

H3 | Concreet: de aanpak van BMC

Voor elk implementatieniveau ondersteunt BMC u bij de borging en verbetering van privacy en informatieveiligheid. De ontwikkeling gebeurt in nauwe samenspraak met uw medewerkers. De inhoudelijke experts van BMC hebben diverse werkvormen ontwikkeld met ondersteuning van hun collega's die gespecialiseerd zijn op het gebied van training en ontwikkeling.

- Scans en assessments om uw situatie in kaart te brengen;
- het opstellen van beleid en onderbouwde keuzes van maatregelen;
- het maken van concrete plannen voor de verdere inrichting in uw organisatie;
- het ondersteunen van en adviseren bij de implementatie.

Implementatieniveau	Diensten Privacy	Diensten Informatiebeveiliging
1. Ad Hoc	<ul style="list-style-type: none"> • Management Workshop • Toetsing aan het privacykader • opstellen van een register van verwerkingen 	<ul style="list-style-type: none"> • Management Workshop • Scan Informatiebeveiliging
2. Basis	<ul style="list-style-type: none"> • Inrichtingsplan beheersingsmaatregelen voor privacy • Toetsing rechtmatigheid van verwerkingen en gegevensuitwisseling • Privacy Impact Assessment 	<ul style="list-style-type: none"> • Opstellen van informatieveiligheidsbeleid • Zelfevaluatie beveiligingsmaatregelen • Dataclassificatie • Risicoanalyse • Plan van aanpak voor implementatie
3. Gepland	<ul style="list-style-type: none"> • Assessment beheersingsmaatregelen (opzet en/of bestaan) • Toetsing rechtmatigheid van verwerkingen en gegevensuitwisseling • Advies en ondersteuning bij implementatie • Privacy Impact Assessment • Training en bewustwording 	<ul style="list-style-type: none"> • Assessment (opzet en/of bestaan) • Risicoanalyse • Implementatieplan • Advies en ondersteuning bij implementatie • Training en bewustwording
4. Geïmplementeerd	<ul style="list-style-type: none"> • Assessment (opzet en bestaan) • Toetsing rechtmatigheid van verwerkingen en gegevensuitwisseling • Advies en ondersteuning bij evaluatie/verbetering • Privacy Impact Assessment 	<ul style="list-style-type: none"> • Assessment (opzet en bestaan), voorbereiding certificeringsaudit • Advies en ondersteuning
5. Pro-Actief	<ul style="list-style-type: none"> • Advies en ondersteuning bij evaluatie/verbetering 	<ul style="list-style-type: none"> • Advies en ondersteuning bij evaluatie/verbetering
Alle niveaus	<ul style="list-style-type: none"> • Training en bewustwording • Privacy Impact Assessments • Jaarlijkse check met verschillende modules: <ul style="list-style-type: none"> - Update verwerkingenregister - Toetsing rechtmatigheid - Evaluatie beheersingsmaatregelen • Interim Functionaris Gegevensbescherming of Privacy expert 	<ul style="list-style-type: none"> • Training en bewustwording • Beveiligingsadviezen • Jaarlijkse checkup met verschillende modules, zoals: <ul style="list-style-type: none"> - Zelfevaluatie - Risico-analyses - Actieplannen • Interim CISO of beveiligingsexpert

Toelichting op de werkvormen

Managementworkshop

In de managementworkshop maken bestuurders en managers kennis met regelgeving rond privacy en informatieveiligheid. Daarmee krijgen zij samen een globale indruk van de actuele situatie van de organisatie. De workshop bestaat een dagdeel en omvat in ieder geval een intake en een rapportage. Naar gelang de situatie kan de workshop gericht zijn op privacy, informatieveiligheid of beide. In de workshop wordt een inventarisatie gemaakt van uw belangrijkste processen, systemen en gegevens. De deelnemers ontdekken de aandachtspunten voor hun organisatie op hoofdlijnen.

Toetsing aan het privacykader

In de privacyevaluatie wordt de verwerking van persoonsgegevens geïnventariseerd en getoetst aan het wettelijk kader van de AVG en andere regels die van toepassing zijn. Het gaat onder andere om: rechtmatigheid van de verwerking (grondslag, doelbinding, proportionaliteit en subsidiariteit), bewaartermijnen, verwerkingsregister, verwerkersovereenkomsten, melding van datalekken, gegevensuitwisseling en informatieveiligheid. Wanneer er nog geen systematische inventarisatie van verwerking van persoonsgegevens heeft plaatsgevonden, kan dit worden opgenomen in het onderzoek.

Assessment beheersing privacy

In het privacyassessment wordt onderzocht welke maatregelen uit de catalogus met beheersmaatregelen voor de AVG in de organisatie in opzet aanwezig zijn. Op basis daarvan wordt er een plan gemaakt voor de verdere implementatie, waarna de organisatie of instelling niet alleen voldoet aan wet- en regelgeving, maar ze kan dit niveau ook in stand houden, aantonen, evalueren en waar nodig verbeteren.

Scan informatieveiligheid

Deze scan is bedoeld voor organisaties die informatieveiligheid nog niet structureel hebben ontwikkeld en geïmplementeerd. De deelnemers leveren op basis van een vragenlijst documenten aan over beleid en maatregelen op het gebied van informatieveiligheid. Deze worden vergeleken met de voor het onderwijs opgestelde normen en de stand van de techniek, en tijdens een beperkt aantal interviews of in een workshop met betrokkenen besproken, bijvoorbeeld verantwoordelijken voor en uitvoerenden van HR-, kwaliteits- en ICT-beleid. Op basis daarvan worden de belangrijkste issues gerapporteerd en worden er vervolgstappen geadviseerd.

Assessment informatiebeveiliging

Voor organisaties die zelf al structureel beleid hebben ontwikkeld en geïmplementeerd zijn er assessments. Daarin worden alle aspecten van informatieveiligheid onderzocht, zoals governance, beleid, organisatorische en technische beveiligingsmaatregelen. In overleg met de opdrachtgever wordt afgesproken of het assessment alleen gaat over de opzet van de beheersingsmaatregelen of dat ook de uitvoering (of het bestaan) van de beheersingsmaatregelen wordt onderzocht. Ook bij een assessment wordt documentonderzoek gecombineerd met interviews, maar het aantal daarvan is groter dan bij een scan. Daarnaast kunnen ook andere vormen van onderzoek worden ingezet, zoals demonstraties en rondleidingen.

Risicoanalyse

Als aanvulling op een scan of een assessment of als basis voor de uitwerking van beleid kan er een risicoanalyse worden uitgevoerd. Daarin worden specifieke bedreigingen voor uw organisatie in kaart gebracht en geeft u zelf een weging aan de risico's, in samenspraak met onze adviseurs. Een risicoanalyse helpt om prioriteiten te stellen, maatregelen te nemen en de restrisico's bewust te accepteren.

Wanneer de organisatie een hoger niveau van volwassenheid heeft bereikt, verschuiven risicoanalyses van organisatiebreed naar procesniveau. Hiermee komen proceseigenaren - en dus lijnverantwoordelijken - verder 'in control' op de specifieke risico's binnen hun verantwoordelijkheidsgebied. Ze kunnen dan ook gedegen afwegingen maken over de implementatie van maatregelen binnen hun processen.

Adequate inrichting van privacy en informatieveiligheid

Op basis van scan, assessment en/of risicoanalyse helpt BMC u om u verder te ontwikkelen en maatregelen te definiëren en te implementeren, zoals:

- het opstellen van een jaar- of meerjarenplan;
- het inrichten van privacy en/of informatieveiligheid;
- het ontwikkelen van beleid;
- implementatie van voor privacy relevante processen en beleid;
- implementatie van managementsystemen, processen en beveiligingsmaatregelen;
- ondersteuning/coaching van verantwoordelijken voor privacy, informatieveiligheid of kwaliteit;
- invulling van de rol van privacy- of informatieveiligheidsbeheerder/- officer in uw organisatie, tijdelijk, parttime of in vaste dienst.

Waarom BMC?

BMC geeft integraal advies door kennis en ervaring van zorg, privacy en informatieveiligheid te combineren. BMC verstaat de taal van verschillende disciplines, van bestuursniveau tot op de werkvloer. BMC neemt de organisatie mee in haar ontwikkeling en stemt haar advies daarop af.

Handige links

- **Algemene Verordening Gegevensbescherming:**
<https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32016R0679&from=EN>
- **Handleiding AVG van de AP**
https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/handleiding_avg.pdf
- **Informatiebeveiliging in het Hoger Onderwijs /MBO**
<https://www.surf.nl/themas/beveiliging/beveiligingsdiensten-en-tools/informatiebeveiliging/index.html>

<https://www.surf.nl/binaries/content/assets/surf/nl/2015/baseline-informatiebeveiliging-ho-2015.pdf>
- **Kennisnet over Informatiebeveiliging in het PO/VO**
<https://www.kennisnet.nl/artikel/wat-is-informatiebeveiliging-en-privacy-en-hoe-regel-ik-dit-op-school/>

https://maken.wikiwijs.nl/81891/Aanpak_IBP_voor_het_PO_en_VO

Contact

Heeft u vragen of wilt u vrijblijvend met ons in contact komen, dan kunt u telefonisch contact opnemen via (033) 496 52 00 of stuur een e-mail.



mr. Alex Commandeur
senior adviseur
06 - 82 12 03 17



ir. Julius Duijts CISSP
senior adviseur
06 - 29 52 55 31

Colofon

Informatiebeveiliging en privacy in het onderwijs - niet meer vrijblijvend
april 2018

Auteurs: mr. Alex Commandeur, senior adviseur
Ir. Julius Duijts CISSP, senior adviseur

Productie: PR & Marketing, BMC

Druk: Randstand Groep Nederland

BMC
Spacelab 4
3824 MR Amersfoort

P.O. box 490
3800 AL Amersfoort

033 - 496 52 00
info@bmc.nl
www.bmc.nl

Kijk voor meer informatie ook eens op onze website www.bmc.nl