

94 normen, één maat?

*Naar een proportionele toepassing van het
Normenkader IBP voor kleine schoolorganisaties*



Opiniestuk door:



Floris Pols



Henk van de Hoef



Samenvatting

Het Normenkader IBP voor het Funderend Onderwijs is een belangrijke stap om digitale veiligheid en privacy structureel op een hoger niveau te brengen. Kleine schoolorganisaties verschillen echter fundamenteel van grote schoolbesturen — niet in de gevoeligheid van de gegevens of de noodzaak om digitaal veilig te werken, maar wél in capaciteit, functiescheiding, technische inrichting en afhankelijkheid van externe leveranciers. Een school met 80 leerlingen, waar de directeur-bestuurder zelf nog voor de klas staat, kan niet op dezelfde manier worden georganiseerd als een groot schoolorganisatie met een eigen ICT-afdeling en stafdiensten.

In het Primair Onderwijs (inclusief VSO) zijn er 325 zogenaamde *eenpitterscholen* en in het Voortgezet Onderwijs 162. Circa 39% van de besturen in het PO en 59% in het VO bestaat uit een op zichzelf staande kleine schoolorganisatie¹. Het gemiddelde leerlingaantal bedraagt in het PO 236 en in het VO 814 leerlingen. 49 van deze scholen in het PO hebben minder dan 100 leerlingen; 42 VO scholen hebben minder dan 500 leerlingen.²

	Primair Onderwijs (PO)	Voortgezet Onderwijs (VO)
Aantal eenpitters	325 (39% van de PO-besturen)	162 (59% van de VO-besturen)
Minimum aantal leerlingen	13	20
Gemiddeld aantal leerlingen	236	814
Minder dan 100 lln (PO) minder dan 500 lln (VO)	49	42

Dat betekent *niet* dat voor kleine schoolorganisaties een lagere veiligheidsambitie zou moeten gelden. Het betekent wél dat er ruimte moet zijn om bewust en aantoonbaar risico's af te wegen. Dit geheel in lijn met art. 32 van de AVG. Ook *Plan Digitaal Veilig Onderwijs* (DVO) en Kennisnet lijken dit te erkennen, gezien de 11 basismaatregelen waarmee iedere school zou moeten beginnen — met hun kanttekening daarbij dat scholen daarmee nog niet aan de volledige norm voldoen.

Onze analyse³ laat zien dat voor kleine schoolorganisaties een serieus deel van de normen op niveau 3 beheerst zouden moeten worden; tenminste 37 van de 69 IB-normen. 32 normen zouden naar onze overtuiging getoetst moeten worden of ze realistisch en voldoende passend zijn voor kleine schoolorganisaties, of dat de uitvoer en borging bij een derde partij ligt. Daarmee pleiten wij *niet* voor minder digitale veiligheid. Ook stellen we niet de noodzaak van (beveiligings)maatregelen ter discussie, maar welk volwassenheidsniveau voor kleine schoolorganisaties passend is en hoe en door wie die maatregelen worden uitgevoerd en geborgd.

¹ Daarnaast kennen we in het Funderend Onderwijs nog 151 Samenwerkingsverbanden, waarvan een fors deel tot een kleine onderwijsorganisatie (< 5 medewerkers op het bestuurskantoor) gerekend zouden moeten worden. Ook zij moeten aan het Normenkader IBP voldoen. Dit pleidooi wordt dus ook voor hen gevoerd.

² Deze cijfers zijn gebaseerd op de leerlingentellingen van DUO van 1 oktober 2025

³ Zie bijlage 1 waar de betreffende normen expliciet worden benoemd

Wij pleiten voor een *adaptief normenkader* waarin naast volwassenheid ook wordt gekeken naar feitelijk risico, proportionaliteit, uitvoerbaarheid en de organisatie die een maatregel daadwerkelijk uitvoert.

Dit lijkt ons geheel in lijn met artikel 32 van de AVG waarin gesteld wordt dat er door de organisatie *passende* technische en organisatorische maatregelen getroffen dienen te worden, rekening houdend met de specifieke omstandigheden en randvoorwaarden.

1. Twee werkelijkheden, één normenkader

Een cyberaanval maakt geen onderscheid tussen een school met 80 leerlingen en een schoolorganisatie met 20.000 leerlingen: leerlinggegevens verdienen overal bescherming en iedere organisatie moet zich bewust zijn van digitale risico's. Tegelijk verschillen de organisaties die deze verantwoordelijkheid dragen enorm.

Aan de ene kant van het spectrum staat een grote schoolorganisatie met een complete staforganisatie, een eigen CISO, Privacy Officer en goed georganiseerde functiescheiding. Aan de andere kant staat de zogenaamde *éénpitter* waar de directeur-bestuurder verantwoordelijk is voor onderwijs, personeel, financiën, huisvesting, privacy én informatiebeveiliging. Diezelfde directeur staat vaak zelf nog voor de klas, terwijl een leerkracht hooguit enkele uren per week ICT-coördinator is, het netwerkbeheer is uitbesteed en bestuurlijke rollen worden ingevuld door vrijwilligers of ouders. Dat laatste is niet per definitie onzorgvuldig; het is de organisatorische werkelijkheid van veel kleine schoolorganisaties.

Het Normenkader IBP stelt voor beide organisaties dezelfde normen. Daar wringt het, maar niet bij iedere norm op dezelfde manier. Voor de privacynormen geldt dat de onderliggende wettelijke verplichtingen uit de AVG in beginsel gelijk zijn voor kleine en grote organisaties. Voor informatiebeveiligingsnormen is naar onze mening meer ruimte voor een risicogestuurde en proportionele toepassing.

De vraag is dus niet óf kleine scholen digitaal veilig moeten zijn, maar wanneer een maatregel toegesneden is op het werkelijke risico. En wanneer wij vooral een organisatorische volwassenheid vragen die een kleine school redelijkerwijs niet kan organiseren. Kan een normenkader, dat voor een grote onderwijsorganisatie logisch is, zonder nadere duiding op precies dezelfde manier worden toegepast op een kleine schoolorganisatie?

Onze conclusie: niet altijd.

2. Het Normenkader IBP is nodig — focus op informatiebeveiligingsnormen

Wij onderschrijven de doelstelling van het Normenkader IBP. Het geeft informatiebeveiliging en privacy een structurele plek, maakt bestuurders bewuster van digitale risico's, creëert een gemeenschappelijke taal, helpt scholen prioriteren en maakt duidelijk dat digitale veiligheid een bestuurlijke verantwoordelijkheid is. We stellen niet de noodzaak van (beveiligings)maatregelen ter discussie, maar welk volwassenheidsniveau voor kleine schoolorganisaties passend is en hoe en door wie die maatregelen worden uitgevoerd en geborgd.

De kern van ons betoog is dus niet: "kleine scholen hoeven minder te doen;" op onderdelen zelfs eerder méér. De kern is: kleine schoolorganisaties moeten de juiste dingen doen en hun beperkte capaciteit inzetten op de risico's die er werkelijk toe doen.

Waarom de 25 privacynormen in dit artikel minder nadruk krijgen

Het Normenkader IBP omvat 69 normen voor informatiebeveiliging en 25 privacynormen. Die laatste krijgen in dit opiniestuk bewust minder nadruk, omdat de onderliggende wettelijke verplichtingen uit de AVG in beginsel voor kleine en grote schoolorganisaties gelijk zijn. Bij enkele privacynormen is een andere

organisatorische invulling en borging ook hier naar onze mening verdedigbaar. [4] Dat doet echter niets af aan de wettelijke verplichtingen: een school kan een inzageverzoek niet minder zorgvuldig behandelen of verplichtingen rond datalekken relativeren omdat de organisatie klein is. De uitvoering kan wél anders worden georganiseerd, bijvoorbeeld via externe ondersteuning of gezamenlijke dienstverlening, maar de school blijft verantwoordelijk voor het nakomen van haar wettelijke privacyverplichtingen.

3. Wanneer wordt een IB-norm disproportioneel?

Informatiebeveiliging draait om risicomanagement: een organisatie identificeert een risico en kan dit verminderen, vermijden of bewust accepteren. Die laatste optie is essentieel voor onze analyse. Wanneer de kans op een incident klein is, de impact beperkt, de benodigde investering groot en andere maatregelen meer risicoreductie opleveren, kan het bestuurlijk verdedigbaar zijn om te zeggen: wij kennen dit risico, hebben het beoordeeld en accepteren — gelet op kans, impact en investering — het restrisico.

Dat is iets anders dan “we doen er niets aan”. Risicoacceptatie is een volwaardige vorm van risicomanagement, mits de afweging bewust plaatsvindt, onderbouwd is, bestuurlijk wordt vastgesteld en periodiek wordt herbeoordeeld. Het bewust accepteren van een lager volwassenheidsniveau is dus niet hetzelfde als het ontbreken van beheersing, maar het resultaat van een aantoonbare risicoafweging: staat de investering die nodig is om naar een hogere volwassenheid te gaan in redelijke verhouding tot de risicoreductie die dat oplevert? Een investering van € 9.000 per jaar kan voor een groot bestuur passend zijn; voor een éénpitter is het dat lang niet altijd.

Voorwaarden voor risicoacceptatie

Een dergelijk besluit mag nooit vrijblijvend zijn. Het bestuur moet minimaal kunnen aangeven:

- welk risico is geïdentificeerd en hoe kans en impact beoordeeld zijn;
- welke maatregelen er al genomen zijn en welke aanvullend mogelijk zouden zijn;
- welke kosten of organisatorische gevolgen dat heeft;
- waarom het restrisico aanvaardbaar wordt gevonden;
- wie het besluit heeft genomen en wanneer het wordt herbeoordeeld.

Niveau 2 accepteren betekent dan niet “we komen niet verder”, maar: “we hebben vastgesteld dat verdere volwassenheid in onze situatie onvoldoende aanvullende risicoreductie oplevert om de investering te rechtvaardigen.” Het kan ook betekenen dat sommige processen nog bewust grotendeels informeel worden uitgevoerd. Dat is een verdedigbare, **volwassen** bestuurlijke keuze.

4 In de bijlage verwijzen we naar vijf privacynormen die evt. op een ander organisatieniveau gerealiseerd kunnen worden, te weten norm O1.02, SW.02, SW.03, VW.01 en PR.06.

4. Twee fictieve praktijkcasussen

In dit kader beschrijven we twee fictieve maar realistische praktijkvoorbeelden, die illustreren waar(om) de proportionaliteitsvraag concreet wordt.



Basisschool De Regenboog (PO, 83 leerlingen)

De Regenboog wordt geleid door directeur-bestuurder Rob, verantwoordelijk voor vrijwel alles — onderwijs, personeel, financiën, huisvesting, privacy én informatiebeveiliging — en zelf nog één dag per week voor de klas. De leerkracht uit groep zes is vier uur per week ICT-coördinator, het bestuur bestaat uit vier ouders en het technisch ICT-beheer is uitbesteed. Het Normenkader vraagt dat processen structureel zijn ingericht, rollen zijn gescheiden en maatregelen aantoonbaar worden beheerst; precies waar directeur Rob en zijn ICT-coördinator geen capaciteit voor hebben. Tegelijk kan hij niet zomaar aannemen dat zijn ICT-leverancier dit wel op orde heeft: de kwaliteit van netwerkbeheerders loopt in de praktijk nogal uiteen en “we hebben het uitbesteed” is op zichzelf geen onderbouwing, mits je het contractueel geborgd hebt. Hoe dat er in de praktijk uit zou kunnen zien, komt in hoofdstuk 5 aan bod.



Oranje College (VO, ± 800 leerlingen)

Het Oranje College heeft wél een eigen IT'er in dienst: Frank, 28 uur per week, met een lokaal ICT-bedrijf als achtervang. Op papier is de capaciteit op Oranje groter dan bij de Regenboog. Maar er ontstaat hier een ander risico: vrijwel alle technische kennis zit bij één persoon (Frank). Bij langdurige ziekte, vertrek of een ernstig incident kan de school een groot probleem hebben. Hier is norm HR.03 (afhankelijkheid van individuen) bijzonder relevant. Extra aandacht voor documentatie, overdraagbaarheid, escalatie en periodieke onafhankelijke controle is dan belangrijker dan verdere formele functiescheiding.

5. Onze analyse van de 69 IB-normen

Wij hebben de 69 IB-normen beoordeeld vanuit de praktijk van kleine schoolorganisaties⁵. Daaruit hebben wij geconcludeerd dat:

- Tenminste 37 normen op niveau 3 dienen te worden gerealiseerd: het risico is simpelweg te groot, te omvangrijk, of de beheersing te essentieel om een lager niveau te moeten willen accepteren: deze normen vormen wat ons betreft de harde kern, ook voor een kleine schoolorganisatie. Hier vallen ook de zogenaamde elf basismaatregelen van Kennisnet onder.
 - Van de overige 32 normen zouden wij ons moeten afvragen:
 - o of ze ook voor kleine schoolorganisaties realistisch en voldoende passend zijn
 - o of de uitvoering en borging niet bij derde partijen ligt (denk aan ict-dienstverleners of leveranciers van SaaS-oplossingen, tbv. de kernapplicaties)
 - o of ze toepasbaar of (beperkt) relevant zijn voor deze kleine organisaties
- Hier is een nadere duiding vanuit het programma Digitaal Veilig Onderwijs (DVO) dringend gewenst.

⁵ Zie bijlage 1 voor een verdere analyse van de betreffende normen

Voorbeeldnormen waar het concreet schuurt

- **OR.02 — Functiescheiding.** Binnen een school waar de directeur-bestuurder vrijwel de gehele bedrijfsvoering draagt, is volwaardige functiescheiding vaak organisatorisch onmogelijk. De relevante vraag is welke alternatieve maatregel voldoende controle biedt (bijvoorbeeld externe controle, een vier-ogenprincipe op risicovolle handelingen of periodieke steekproeven).
- **CO.02, CH.04–06 — Testomgevingen en promotie naar productie.** Deze normen passen bij organisaties die zelf systemen ontwikkelen of beheren, of zelf workflows maken in bv. het personeelsadministratiesysteem. Veel kleine scholen gebruiken alleen standaard cloudsoftware; voor hen zouden deze normen goeddeels naar leveranciersmanagement moeten verhuizen.
- **OP.03 — Capaciteitsbeheer.** Relevant wanneer een organisatie zelf infrastructuur beheert, maar hoe reëel is dat risico bij een school die geen eigen server heeft en vrijwel volledig cloudgebaseerd werkt? De feitelijke technische situatie moet bepalend zijn voor de zwaarte van de norm.

Deze voorbeelden laten telkens hetzelfde zien: de beveiligingsmaatregel is terecht, terwijl de voorgeschreven volwassenheid niet of onvoldoende aansluit bij de werkelijkheid van een kleine schoolorganisatie. Dat geldt evengoed voor uitbestedde techniek. Uitbesteding verandert wie de maatregel uitvoert (denk aan onderhoud van kernapplicaties, endpointbeheer, patchmanagement, back-up en monitoring), maar niet wie ervoor verantwoordelijk blijft, namelijk: de school. Een schoolbestuur kan daarom niet volstaan met het antwoord “het is uitbesteed”, maar moet kunnen aantonen welke maatregelen bij de leverancier zijn belegd, welke eisen en afspraken daarvoor gelden en hoe een en ander periodiek wordt beoordeeld.⁶

6. Van norm naar proportionele beheersing

Wij stellen daarom voor om bij iedere IB-norm de onderstaande *zeven vragen* te doorlopen:

1. welk risico wordt beheerst;
2. hoe relevant is dat risico voor deze organisatie;
3. wie beheerst het risico;
4. wie bepaalt welke beheersing noodzakelijk is;
5. hoe wordt het restrisico beoordeeld;
6. welk volwassenheidsniveau is proportioneel en
7. welke bewijslast past daarbij.

Op basis daarvan kan worden bepaald wie de maatregel uitvoert, hoe deze organisatorisch wordt ingericht, welke externe ondersteuning nodig is en hoe naleving wordt aangetoond. Het wettelijk vereiste resultaat zelf blijft echter gelijk.

⁶ Denk aan het opvragen van een periodieke rapportage of certificering of een jaarlijkse onafhankelijke toets.

7. Drie gerichte oproepen

Oproep 1 — Aan Plan DVO en de sectorraden

Aan PO-Raad, VO-raad, Kennisnet, SIVON en OCW vragen we: kom met handreikingen specifiek voor kleine schoolorganisaties. Het normenkader biedt nu te weinig expliciete ruimte om op basis van risico, proportionaliteit en organisatorische context gemotiveerd te kiezen voor een ander volwassenheidsniveau. Neem hun feitelijke risico's als vertrekpunt, formuleer criteria waaronder een lager volwassenheidsniveau bestuurlijk verdedigbaar is, erken dat meerdere rollen in één persoon kunnen samenkomen, geef aan welke alternatieve maatregelen mogelijk zijn wanneer functiescheiding niet haalbaar is, maak expliciet wanneer en onder welke voorwaarden een ander niveau aanvaardbaar is, of een norm zelfs niet van toepassing blijkt te zijn, welke beheersing bij leveranciers kan worden belegd en erken een proportionele vorm van risicoacceptatie.

Oproep 2 — Aan netwerkbeheerders, (applicatie)leveranciers en ICT-dienstverleners

Aan dienstverleners vragen we: maak zichtbaar wat jullie voor scholen regelen: welke IB-normen jullie voor scholen uitvoeren en borgen, op welk volwassenheidsniveau en onder welke contractuele voorwaarden dat gebeurt. Maak daarbij ook expliciet welke verantwoordelijkheden bij het schoolbestuur zelf blijven liggen. Ontwikkel (liefst collectief) een gestandaardiseerde IBP-verantwoordelijkheids- en assurance matrix, zodat niet honderden scholen afzonderlijk dezelfde vragen hoeven te stellen aan dezelfde netwerkbeheerders, ICT-dienstverleners en applicatieleveranciers.

Oproep 3 — Aan de kleine schoolorganisaties zelf

Een pleidooi voor proportionaliteit is geen reden om af te wachten. Breng als kleine schoolorganisatie of samenwerkingsverband uw belangrijkste (digitale) risico's in beeld, weet welke maatregelen uw netwerkbeheerder uitvoert en spreek leveranciers daarop aan, leg afspraken en risicoacceptaties expliciet vast, kijk kritisch naar afhankelijkheid van individuele medewerkers en behandel de privacynormen als wettelijke verplichting. Bundel waar mogelijk de krachten: via samenwerking met andere kleine besturen, gezamenlijke inkoop, gedeelde audits of verdere uitbesteding aan professionele dienstverleners.



Conclusie

Het Normenkader IBP is een belangrijke ontwikkeling voor het funderend onderwijs. Maar de kracht van een normenkader wordt niet bepaald door de vraag of iedere organisatie hetzelfde volwassenheidsniveau behaalt; de relevante vraag is of risico's daadwerkelijk worden beheerst. Een basisschool met 80 leerlingen, een VO-school met één systeembeheerder en een grote schoolorganisatie met een professionele ICT-afdeling dragen allemaal verantwoordelijkheid, maar hebben niet hetzelfde risicoprofiel, dezelfde capaciteit of dezelfde mogelijkheden om IBP-maatregelen te organiseren. Vanuit de AVG hoeft dit ook niet: een school dient (bij de school) *passende* technische en organisatorische maatregelen te nemen.

Daarom stellen wij voor om bij de beoordeling van de 69 IB-normen náást de norm zelf expliciet te kijken naar risico, context, uitvoering, volwassenheid en bewijslast. Wij roepen *Plan Digitaal Veilig Onderwijs* op om voor kleine schoolorganisaties duidelijke handreikingen voor proportionaliteit, gelijkwaardige maatregelen, uitbestede beheersing en passend bewijslast te ontwikkelen, netwerkbeheerders op om transparant te maken welke maatregelen zij voor scholen uitvoeren en op welk niveau, en kleine schoolbesturen op om het normenkader serieus te nemen en hun risico's bewust te wegen.

Het doel is niet dat iedere school 69 keer een drie invult. Het doel is dat iedere bestuurder kan uitleggen: dit zijn onze belangrijkste risico's. Dít hebben wij eraan gedaan, dít doet onze leverancier, dit restrisico accepteren wij bewust, onze wettelijke privacyverplichtingen komen wij na en dit is hoe onze leerlingen, medewerkers en organisatie verantwoord worden beschermd.

Dat is geen verlaging van de lat. Dat is volwassen risicomanagement én wettelijke naleving.

Over de auteurs:



Floris Pols is directeur van **SecureWave** en adviseur Informatiebeveiliging. Hiervoor was hij lid van de klankbordgroep Digitale Veiligheid van de VO-Raad en CISO van Stichting BOOR te Rotterdam.



Henk van de Hoef is directeur van **Privacy op School** en sinds 1996 vanuit diverse rollen werkzaam op het snijvlak van onderwijs en digitalisering.



Bijlage:

overzicht van de normen waarbij een adaptieve invulling nodig is.

