IBP in beeld

Een verkenning van het volwassenheidsniveau van het Normenkader Informatiebeveiliging en Privacy voor het onderwijs

Ministerie van Onderwijs, Cultuur en Wetenschap

Kennisnet

SIVON

PO RAAD

VO RAAD

Inhoudsopgave

Managementsamenvatting

Deze verkenning geeft een eerste sectorbreed beeld van de voortgang van schoolbesturen in het primair en voortgezet onderwijs ten opzichte van het Normenkader Informatiebeveiliging en Privacy (IBP). In totaal is data van 485 schoolbesturen meegenomen in deze verkenning. Dit komt neer op ongeveer 40% van de sector. De data is afkomstig uit zelfevaluaties.

GEMIDDELD VOLWASSENHEIDSNIVEAU

Het gemiddelde volwassenheidsniveau bedraagt op een schaal van 1 tot 5:

- Totaal: 1,7
- Informatiebeveiliging: 1,5
- Privacy: 1,9

Voor informatiebeveiliging behaalt op dit moment nog geen enkel bestuur een gemiddeld volwassenheidsniveau van 3, het streefniveau binnen het Normenkader IBP. Voor privacy ligt dat anders. Daar wordt dit volwassenheidsniveau door sommige scholen al wel gehaald. De gemiddelde volwassenheid voor het privacy-onderdeel ligt dan ook iets hoger dan die voor informatiebeveiliging. Privacy is voor veel schoolbesturen een bekend thema, onder meer door de aandacht die de Algemene Verordening Gegevensbescherming (AVG) vraagt en de maatregelen die daaruit volgen.

De uitkomsten van deze verkenning passen bij het beeld dat de implementatie van het Normenkader IBP zich binnen het funderend onderwijs nog in een ontwikkelfase bevindt. Schoolbesturen hebben desondanks doorgaans wel zicht op wat nodig is om het normenkader te implementeren. Dit wordt onder andere bevestigd in de Monitor Digitalisering Onderwijs 2025[1]. Hier geven besturen en beleidsmedewerkers aan vooral behoefte te hebben aan extra capaciteit en budget voor de uitvoering en in mindere mate aan aanvullende kennis.

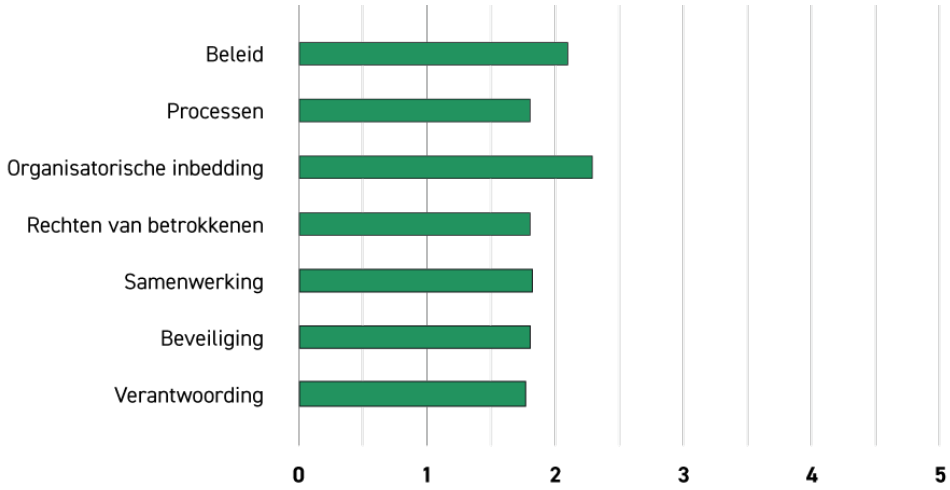
1 **Landelijke rapportage Monitor Digitalisering Onderwijs 2025 - Onderzoeksrapportage digitalisering in het funderend onderwijs 2025**. De MDO schetst een landelijk beeld van de stand van digitalisering in het primair, gespecialiseerd en voortgezet onderwijs, inclusief gebruik, ervaringen, randvoorwaarden, ambities en actuele thema's zoals AI, ethiek en open leermaterialen. Het laat daarbij verschillen zien tussen sectoren, schooltypes, regio's en schoolgroottes.

BEGINFASE VAN VOLWASSENHEID

De resultaten laten zien dat de sector zich grotendeels bevindt in de beginfase van volwassenheid (niveau 1–2). Dat betekent dat de implementatie van het normenkader veelal is gericht op beleidsvorming en organisatorische inrichting. Binnen informatiebeveiliging liggen de volwassenheidsniveaus voor domeinen als Systeemontwikkeling, Changemanagement en Bedrijfscontinuïteitsmanagement relatief lager dan bij de andere IB-domeinen. Voor privacy liggen de volwassenheidsniveaus voor de meeste domeinen op een onderling vergelijkbaar niveau, met uitzondering van de domeinen Organisatorische inbedding en Beleid. Deze twee domeinen scoren net boven niveau 2 en daarmee iets hoger dan de andere privacydomeinen.

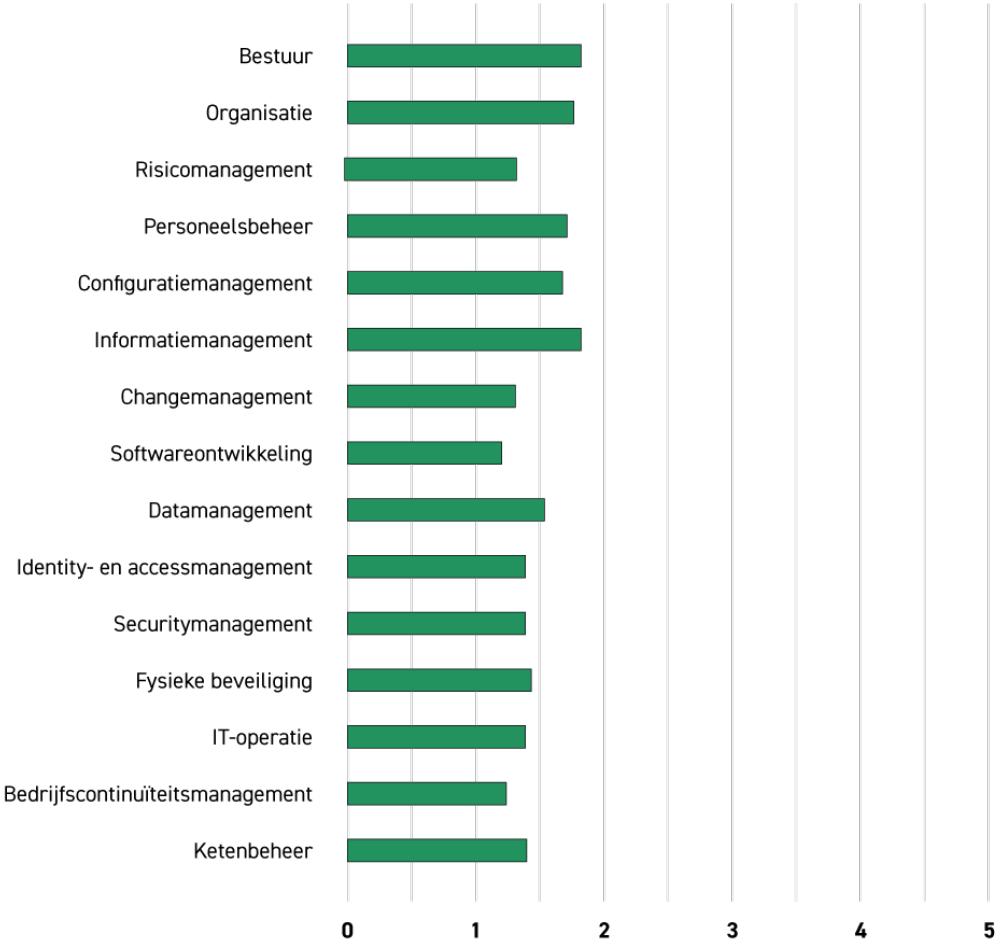
Privacy

Grafiek 1 Score per privacydomein[2]



Informatiebeveiliging

Grafiek 2 Score per informatiebeveiligingsdomein



2 Primair, gespecialiseerd en voortgezet onderwijs, inclusief gebruik, ervaringen, randvoorwaarden, ambities en actuele thema's zoals AI, ethiek en open leermaterialen. Het laat daarbij verschillen zien tussen sectoren, schooltypes, regio's en schoolgroottes.

ONDERWIJSSOORT

De verschillen tussen de onderwijssoorten (primair, voortgezet en gespecialiseerd onderwijs) zijn over het algemeen beperkt. In alle sectoren ligt de gemiddelde volwassenheid voor informatiebeveiliging lager dan voor privacy. Het voortgezet onderwijs (VO) laat binnen dit onderzoek de hoogste gemiddelde scores zien voor zowel de totaalscore als voor informatiebeveiliging en privacy. Voor het gespecialiseerd onderwijs (GO) en de samenwerkingsverbanden geldt dat het aantal besturen waarvan data beschikbaar was beperkt is. Hierdoor geven de resultaten voor deze groepen een selectief sectorbeeld en moeten ze met enige terughoudendheid worden geïnterpreteerd.

Tabel 1 Gemiddeld volwassenheidsniveau voor IBP

Aantal per onderwijssoort	Gemiddelde score
Primair onderwijs	1,6
Voortgezet onderwijs	1,7
Gespecialiseerd onderwijs	1,7
Gemengde besturen[3]	1,6
Samenwerkingsverbanden	1,4

OMVANG

Voor de omvang van de besturen is gekeken naar het aantal leerlingen per schoolbestuur. Daaruit blijkt dat bij grotere besturen waar meer leerlingen onder vallen de volwassenheid hoger is. De schoolbesturen met het hoogste aantal leerlingen scoren gemiddeld het hoogst (2,0). De overige categorieën liggen dicht bij elkaar qua scores. Dit past bij de aanname dat grotere schoolbesturen meer capaciteit en expertise hebben op dit onderwerp en daarmee beter in staat zijn om het Normenkader IBP te implementeren.

Tabel 2 Gemiddeld volwassenheidsniveau voor IBP

Aantal leerlingen per bestuur	Gemiddelde score
0-1.000	1,5
1.000-5.000	1,6
5.000-10.000	1,7
10.000+	2,0

3 Gemengde besturen bieden verschillende onderwijssoorten aan.

REGIO

De regionale verschillen zijn klein. Daarmee is de regio de minst bepalende factor voor de hoogte van het volwassenheidsniveau. Regio Zuid en Noord scoren beide iets lager (1,6) dan Midden, maar het verschil is beperkt (ongeveer 0,1).

WAARDE VAN DE RESULTATEN

De resultaten van deze verkenning moeten met enige voorzichtigheid worden geïnterpreteerd. Het betreft een zelfevaluatie zonder externe validatie, met beperkte representativiteit voor sommige onderwijssoorten en voor kleine besturen. Doordat alleen gebruik is gemaakt van data uit zelfevaluaties is enkel gekeken naar de opzet van maatregelen, maar niet naar de toepassing en werking ervan. De resultaten geven daarmee weliswaar een indicatief beeld, maar geen volledig representatief sectorbeeld.

1. Inleiding

Schoolbesturen rapporteren sinds 2024 in hun jaarverslag over digitale veiligheid en hun aanpak van informatiebeveiliging en privacy. Daarnaast maakt digitale veiligheid onderdeel uit van het intern toezicht. Het Normenkader Informatiebeveiliging en Privacy (IBP) geeft scholen richting bij het verbeteren van hun digitale veiligheid en het beschermen van persoonsgegevens.

Het normenkader beschrijft de eisen waar scholen aan moeten voldoen om te zorgen voor een veilige digitale leer- en werkomgeving en welke volwassenheidsniveaus daarin te onderscheiden zijn. Het ministerie van Onderwijs, Cultuur en Wetenschap (OCW) heeft met de PO-Raad en VO-raad afgesproken dat alle schoolbesturen vanaf 2027 inzicht hebben in waar ze staan ten opzichte van het normenkader en dat zij een plan hebben uitgewerkt om aan alle normen te voldoen. Vanaf 2030 dienen schoolbesturen daadwerkelijk aan de normen uit het normenkader te voldoen. Daarnaast verkent het ministerie de mogelijkheden om de bevoegdheid van de Inspectie van het Onderwijs ten aanzien van het toezicht en interventie op digitale veiligheid vast te leggen.

SECTORBREDE NULMETING

Tegen deze achtergrond is het waardevol om sectorbrede inzichten te verzamelen. Deze verkenning biedt een eerste beeld van waar schoolbesturen staan ten opzichte van de normen uit het Normenkader IBP. Het is daarmee een vervolg op de Nulmeting Normenkader IBP FO[4] uit 2023. Daar deden destijds 15 schoolbesturen aan mee, waardoor er nog geen stevige sectorbrede nulmeting kon worden neergezet. De huidige verkenning bevat data van veel meer schoolbesturen, maar voor een representatieve benchmark is meer onderzoek en een uitgebreidere dataset nodig.

4 Nulmeting Normenkader IBP FO (2023)

VERSTERKEN DIGITALE WEERBAARHEID

In 2026 zal opnieuw een sectorbeeld worden opgesteld op basis van data uit zelfevaluaties. Om te zorgen voor een betere kwaliteit en representativiteit van de data wordt er gewerkt aan een vast programma van eisen voor de volgende data-uitvraag. Daarnaast wordt er onderzocht hoe er vanaf 2027 een structureler sectorbeeld kan worden opgesteld dat kan functioneren als een representatieve benchmark voor informatiebeveiliging en privacy in het funderend onderwijs.

In de tussentijd draagt deze verkenning bij aan het versterken van de digitale veiligheid in het funderend onderwijs. Het biedt inzicht in waar schoolbesturen staan ten opzichte van het Normenkader IBP en ondersteunt hen bij het verder versterken van hun digitale weerbaarheid. Het sectorbeeld kan daarbij helpen door:

- Inzicht te geven in overeenkomsten en verschillen binnen de sector, waardoor besturen hun eigen situatie beter kunnen duiden.
- Gerichtere ondersteuning en hulpmiddelen aan te bieden vanuit het programma Digitaal Veilig Onderwijs (DVO)[5].

Over het Normenkader IBP

Het Normenkader Informatiebeveiliging en Privacy (IBP) ondersteunt scholen bij het verbeteren van hun digitale veiligheid en het beschermen van persoonsgegevens. Het normenkader is door Kennisnet ontwikkeld in samenwerking met het ministerie van OCW, SIVON, de PO-Raad en de VO-raad. Het Normenkader IBP bevat in totaal 94 normen: 69 voor informatiebeveiliging en 25 voor privacy:

- De normen voor **informatiebeveiliging** gaan over de bescherming van de organisatie en alle vormen van informatie.

- De normen voor **privacy** gaan over de bescherming van persoonsgegevens van leerlingen, ouders en medewerkers en vloeien voort uit de Algemene Verordening Gegevensbescherming (AVG).

Groeipad

In het Normenkader IBP is per norm uitgewerkt wat er van een schoolbestuur wordt verwacht en welke maatregelen daarbij horen, uitgewerkt naar verschillende volwassenheidsniveaus. Het programma DVO heeft het Groeipad ontwikkeld om schoolbesturen te helpen bij het implementeren van normen. Het Groeipad bundelt normen op een logische manier in deelprojecten en helpt zo scholen gestructureerd en stapsgewijs naar het gewenste volwassenheidsniveau.[6]

Volwassenheidniveaus

Het Normenkader IBP werkt met vijf volwassenheidsniveaus per norm: van niveau 1 tot en met 5.[7] De volwassenheidsniveaus helpen schoolbesturen om te bepalen waar zij staan ten opzichte van de normen in het normenkader en welke aanvullende maatregelen nodig zijn om te groeien in volwassenheid. Hoe hoger het niveau, hoe beter systemen en persoonsgegevens zijn beschermd en hoe kleiner de kans op datalekken, cyberaanvallen en privacyschendingen. Niveau 3 is het minimum waar de sector naar streeft.[8] Zijn besturen al verder met IBP? Dan kunnen ze doorgroeien naar niveau 4 en 5. Bekijk de bijlage voor meer uitleg over alle volwassenheidsniveaus.

5 Over programma Digitaal Veilig Onderwijs | Digitaal Veilig Onderwijs

6 Groeipad | Normenkader IBP

7 Inhoud en opzet van het Normenkader IBP | Normenkader IBP

8 Digitaal veilig onderwijs vraagt nu actie van schoolbesturen | Ministerie van OCW en Kamerbrief over digitale veiligheid in het funderend onderwijs | Rijksoverheid.nl

2. Methodologische verantwoording en beperkingen

Er zijn verschillende methoden mogelijk om de volwassenheid van schoolbesturen in kaart te brengen. Grofweg zijn dat de interne audit of zelfevaluatie, de externe audit en peer review.[9] Voor deze verkenning is ervoor gekozen gebruik te maken van data die afkomstig is uit zelfevaluaties. Al deze zelfevaluaties zijn inhoudelijk gebaseerd op het Normenkader Informatiebeveiliging en Privacy voor het onderwijs.

De verkenning is opgesteld aan de hand van:

- **Kwantitatieve data.** De kwantitatieve data is verzameld tussen 24 december 2025 en 16 januari 2026 en afkomstig van drie leveranciers van Governance, Risk en Compliance (GRC) tools en van de de tool Zelfevaluatie Normenkader IBP.[10]
- **Kwalitatieve data.** Daarnaast hebben we gebruikgemaakt van het rapport Monitor *Digitalisering Onderwijs* (2025)[11] en van het rapport *Digitale weerbaarheid en veiligheid*[12].

KWALITEIT EN BETROUWBAARHEID VAN DE CIJFERS

Voor deze verkenning is gekeken naar de kwaliteit en betrouwbaarheid van de gebruikte cijfers. Voor zowel de GRC-tool als de tool Zelfevaluatie Normenkader IBP is gebruikgemaakt van hetzelfde format: het Normenkader IBP. Scores zijn op basis van dit format ingevuld. Daarmee is de inhoudelijke basis van de meting voor iedereen hetzelfde. De betrouwbaarheid van de cijfers zelf is echter beperkt.
Dit heeft een aantal redenen:

- Heeft een school zelf nog niks ingevuld bij het volwassenheidsniveau van een norm? Dan vullen sommige GRC-tools standaard een 1 in. In overleg met leveranciers is daarom de aanname gedaan dat als een schoolbestuur bij alle normen van het deel informatiebeveiliging of bij alle normen van het deel privacy een 1 heeft staan, de zelfevaluatie als niet ingevuld wordt beschouwd. Deze resultaten zijn in dat geval verwijderd en niet meegenomen in de verdere analyse. Mogelijk komt het gemiddelde eindcijfer binnen deze verkenning iets hoger uit dan in werkelijkheid het geval is.
- Bij de zelfevaluatie is vooral gekeken naar de opzet van processen: zijn processen beschreven en ingericht? Er is echter niet vastgesteld of deze processen ook daadwerkelijk bestaan. Functioneren ze bijvoorbeeld in de praktijk? Of werken ze zoals bedoeld? Zijn ze bijvoorbeeld over een langere periode effectief? De meting geeft dus vooral inzicht in de opzet van maatregelen en minder in het bestaan en de werking ervan.
- Omdat het gaat om een zelfevaluatie, kunnen verschillen ontstaan in de manier waarop schoolbesturen hun volwassenheidsniveau inschatten. Dit kan leiden tot variaties in de scores, afhankelijk van hoe normen worden geïnterpreteerd en beoordeeld.

9 Zelfevaluatie: een interne IT-auditor of functionaris met IT-affiniteit voert de evaluatie uit. Peer review: een andere instelling controleert jouw zelfevaluatie en bewijslast (en andersom). Externe audit: een onafhankelijke auditor geeft een onafhankelijk oordeel. Zie ook: SURFaudit FAQ - Security Expertise Centrum | by SURF

10 Zelfevaluatie Normenkader IBP | wijzer.kennisnet.nl

11 Monitor Digitalisering Onderwijs 2025: kloof tussen beleid en praktijk | Kennisnet

12 Rapport Monitor digitale weerbaarheid en veiligheid | Inspectie van het onderwijs

- De sector funderend onderwijs is een complexe sector, met grote verschillen in onderwijssoorten, schaalgrootte en onderlinge relaties in bijvoorbeeld samenwerkingsverbanden. Daarmee is het lastig om een uniform beeld te geven van de volwassenheid van de gehele sector.
- Tot slot geldt dat de uitkomsten vooral betrekking hebben op het reguliere primair onderwijs (basisscholen) en het voortgezet onderwijs (middelbare scholen), omdat voor deze onderwijssoorten voldoende data beschikbaar is. Voor onderwijssoorten als het gespecialiseerd onderwijs, gemengd onderwijs en samenwerkingsverbanden is het aantal besturen in de dataset beperkt. Daardoor kunnen over deze groepen geen of slechts zeer beperkte uitspraken worden gedaan.

ANALYSE VAN AFWIJKINGEN

De afwijkingen in de resultaten van deze verkenning zijn geanalyseerd op basis van de Benchmark MBO en op basis van expertreviews.

Benchmark MBO

Binnen het MBO wordt een jaarlijkse benchmark uitgevoerd in samenwerking met SURFaudit. Uit deze benchmark[13] blijkt dat de gemiddelde scores in het MBO hoger liggen voor zowel informatiebeveiliging (2,2 ten opzichte van 1,5) als privacy (2,4 ten opzichte van 1,9) dan in het primair en voortgezet onderwijs. Dit verschil is onder andere te verklaren door het feit dat MBO-instellingen meer capaciteit en expertise in huis hebben voor informatiebeveiliging en privacy. Daarnaast startte in het MBO de sectorbrede aanpak van informatiebeveiliging en privacy in 2014 met de oprichting van de Taskforce IBP. Sindsdien wordt jaarlijks een benchmark uitgevoerd. Hierdoor heeft het MBO meer tijd gehad om informatiebeveiliging en privacy te organiseren en meer ervaring opgedaan met benchmarking.

13 Benchmark IBP 2025: 'Mbo-sector groeit in volwassenheid, maar de cijfers laten dat niet altijd zien' | MBO Digitaal

Expertreviews

Naast de data van de drie GRC-leveranciers en de tool Zelfevaluatie Normenkader IBP zijn een beperkt aantal expertreviews uitgevoerd. Zo heeft SIVON een onafhankelijke beoordeling uitgevoerd van de zelfevaluatie van vier schoolbesturen. Daarbij is voor 16 van de 94 normen beoordeeld in hoeverre de ingevulde normen en onderbouwingen aansluiten bij de documentatie en de feitelijke werkwijze binnen de organisatie. De score van drie van de vier schoolbesturen kwam overeen met de score die uit de expertreview kwam. Het kleine aantal expertreviews en de beperkte omvang ervan maakt het echter lastig om hieruit af te leiden dat scholen hun eigen volwassenheid goed in kunnen schatten bij een zelfevaluatie.

3. Representativiteit van de data

In totaal deden er 485 besturen mee aan deze verkenning. 446 besturen namen deel via één van de drie GRC-tools en 39 besturen via de tool Zelfevaluatie Normenkader IBP. De data uit de GRC-tools hebben we ontvangen van de GRC-leveranciers. De data uit de zelfevaluatietool hebben we rechtstreeks via de besturen verzameld.

Het primair en voortgezet onderwijs bestaat uit iets meer dan 1.100 besturen[14].
De data van ongeveer 40% daarvan is gebruikt voor deze verkenning.

- Een groot deel van de data waar deze verkenning op gebaseerd is, is afkomstig van besturen uit het **primair onderwijs** (308 schoolbesturen). Hiermee worden meer dan 500.000 leerlingen vertegenwoordigd.
- Het **voortgezet onderwijs** wordt vertegenwoordigd door 166 schoolbesturen. Hier vallen meer dan 300.000 leerlingen onder.
- Data van 3 schoolbesturen is afkomstig van besturen die alleen **gespecialiseerd onderwijs** aanbieden. Omdat gespecialiseerd onderwijs aangeboden kan worden door scholen die ook regulier onderwijs aanbieden, is niet goed te zeggen hoe deze onderwijssoort vertegenwoordigd is. Er zijn 8 **samenwerkingsverbanden** vertegenwoordigd door de data. De resultaten van die categorie zijn daarmee niet representatief voor deze onderwijssoort.
- De omvang van de besturen in deze verkenning is gebaseerd op het aantal leerlingen. Besturen met **minder dan 1.000 leerlingen** vormen 22% van de dataset en zijn daarmee relatief beperkt vertegenwoordigd. Het grootste aandeel bestaat uit **besturen met 1.000 tot 5.000 leerlingen** (58%). **Besturen met 5.000 tot 10.000 leerlingen** vormen 15% van de dataset en **besturen met meer dan 10.000 leerlingen** 6%.

14 Open onderwijsdata | Duo.nl

Tabel 3 Aantal leerlingen per bestuur per onderwijssoort in absolute aantallen en percentages. Er kan sprake zijn van afrondingsverschillen in de percentages.

Leerlingen	0–1.000	1.000–5.000	5.000–1.0000	1.0000+	Totaal
Gemengd onderwijs	3 (1%)	10 (2%)	5 (1%)	0	18 (4%)
Primair onderwijs	78 (16%)	171 (35%)	46 (10%)	13 (3%)	308 (64%)
Gespecialiseerd onderwijs	0	3 (1%)	0	0	3 (1%)
Samenwerkingsverbanden	8 (2%)	0	0	0	8 (2%)
Voortgezet onderwijs	16 (3%)	99 (20%)	12 (4%)	12 (3%)	148 (30%)
Eindtotaal	**105 (22%)**	**283 (58%)**	**72 (15%)**	**25 (6%)**	**485 (100%)**

GRC-LEVERANCIERS

Voor deze verkenning naar het IBP-volwassenheidsniveau van schoolbesturen hebben we gebruikgemaakt van data van een aantal GRC-leveranciers. GRC staat voor Governance, Risk en Compliance. Dit zijn softwareoplossingen om IBP-documentatie en maatregelen in bij te houden. De tools kunnen ook gebruikt worden om te voldoen aan de verantwoordingsplicht.

4. Resultaten informatiebeveiliging

Het Normenkader IBP bestaat uit 2 onderdelen: informatiebeveiliging en privacy. Die onderdelen bestaan op zichzelf weer uit verschillende domeinen. De domeinen hebben allemaal een eigen set aan normen. Bij de beschrijving van de resultaten houden we deze onderverdeling aan. We gaan hier dieper in op de resultaten voor informatiebeveiliging. Informatiebeveiliging bestaat uit 15 domeinen en 69 normen.

Elke norm heeft 5 volwassenheidsniveaus. Per volwassenheidsniveau staan de maatregelen opgesomd die je genomen moet hebben om aan dat niveau te voldoen. Om te illustreren wat een specifieke score op een domein of norm betekent, geven we bij de resultaten hieronder voorbeelden van welke maatregelen behorende bij een norm wel of niet genomen zijn. Dit geldt dus niet voor elk schoolbestuur uit de dataset, maar is een generalisatie op basis van de gemiddelde score.

HOOGST SCORENDE DOMEINEN

De hoogst scorende domeinen binnen informatiebeveiliging zijn:

- Organisatie (1,8)
- Bestuur (1,9)

We gaan hieronder in op specifieke bevinden bij deze domeinen.

Domein Organisatie

Een van de best scorende domeinen binnen IB is het domein Organisatie, maar met een score van 1,8 is ook dit domein nog niet op het volwassenheidsniveau 3 geïmplementeerd. Hierbij valt op dat norm OR.01 Eigenaarschap, rollen, verantwoordelijkheden en aansprakelijkheid gemiddeld hoger scoort dan OR.02 Functiescheiding. In de praktijk betekent dit het volgende:

- Schoolbesturen zijn bezig met het beleggen van eigenaarschap, rollen en verantwoordelijkheden. Dit is een belangrijke stap voor het implementeren van het normenkader en is ook een van de eerste stappen van het Groeipad.
- De meeste schoolbesturen hebben de cruciale rollen voor informatiebeveiliging en risicomanagement inmiddels ingevuld.
- Functiescheiding is bij veel schoolbesturen nog beperkt ingericht. De bijbehorende norm (OR.02 Functiescheiding) valt in het Groeipad onder een latere fase van volwassenheid. Daarnaast kan het voor kleinere schoolbesturen, bijvoorbeeld wanneer één persoon verantwoordelijk is voor meerdere taken rondom digitalisering, lastig zijn om functiescheiding volledig te realiseren.

Domein Bestuur

Binnen het domein Bestuur zie je dat de normen GO.01 Strategie informatiebeveiliging en GO.02 Beleid informatiebeveiliging boven de 2.0 scoren en GO.03 Planning/roadmap informatiebeveiliging rond de 1,9. De overige normen - GO.04 Informatiearchitectuur en GO.05 Onafhankelijke toetsing - blijven nog achter. In de praktijk betekent dit het volgende:

- Veel schoolbesturen hebben een strategie en visie opgesteld, maar deze is wellicht nog niet altijd vastgesteld of gecommuniceerd binnen de organisatie.
- Schoolbesturen hebben beleid opgesteld rondom informatiebeveiliging. Dit beleid zal echter nog niet in alle gevallen uitgevoerd en geëvalueerd worden.
- Schoolbesturen zijn bezig met het opstellen van een roadmap voor het inrichten van hun informatiebeveiliging.
- Het werken volgens een architectuur is nog complex voor veel schoolbesturen en staat nog in de kinderschoenen.
- Schoolbesturen maken nog zeer beperkt gebruik van onafhankelijke toetsing. De bijbehorende norm hiervoor (GO.05 Onafhankelijke toetsing) valt ook onder een latere fase in het Groeipad, dus implementatie hiervan zal bij veel schoolbesturen nog niet gebeurd zijn.

LAAGST SCORENDE DOMEINEN

De laagst scorende domeinen binnen informatiebeveiliging zijn:

- Systeemontwikkeling (1,3)
- Bedrijfscontinuïteitsmanagement (1,3)

We gaan hieronder in op specifieke bevinden bij deze domeinen.

Domein Systeemontwikkeling

Het laagst scorende domein binnen IB is het domein Systeemontwikkeling. Dit domein beschrijft normen over het veilig ontwikkelen van software, het toepassen van security en privacy by design bij softwareontwikkeling en datamigratie en/of -conversie. Deze normen komen terug in fase 4 en 5 van het Groeipad.

Veel schoolbesturen geven aan dat de normen SD.01 Methodiek veilige softwareontwikkeling en -implementatie en SD.02 Toegang productieomgeving door ontwikkelaars niet van toepassing zijn. Deze zijn daarom uitgesloten van de analyse voor deze verkenning. Mogelijk heeft een deel van de schoolbesturen ervoor gekozen de normen te markeren met volwassenheidsniveau 1 in plaats van 'niet van toepassing', waardoor de score is vertekend. Voor schoolbesturen die wél zelf software ontwikkelen, betekent deze lage score in de praktijk:

- Systeem en softwareontwikkeling gebeurt ad hoc.
- Schoolbesturen die software ontwikkelen hebben geen beleid voor toegangsrestricties door ontwikkelaars.
- Er worden geen of weinig maatregelen genomen voor het waarborgen van de kwaliteit van data als er datamigratie en/of conversie plaatsvindt.

Domein Bedrijfscontinuïteitsmanagement

Een ander laag scorend domein binnen IB is het domein Bedrijfscontinuïteitsmanagement. Dit domein bevat normen die gaan over het voorbereid zijn op grote verstoringen, het inrichten en testen van processen om snel weer aan de slag te gaan na grote verstoringen en het inrichten van crisismanagement. Deze normen komen terug in fase 2 van het groeipad.

Het achterblijven in volwassenheid op deze normen betekent in de praktijk het volgende:

- Continuïteitsplannen zijn beperkt beschikbaar en worden niet of ad-hoc getest.
- De continuïteit van het onderwijs komt mogelijk in het geding bij een grote verstoring. Mogelijk zijn er ad-hoc afspraken gemaakt met leveranciers, maar bij de meeste schoolbesturen is hier geen proces voor ingericht.
- Schoolbesturen zijn beperkt bezig met het oefenen van hun processen en crisismanagement.

Algemene bevindingen informatiebeveiliging

Wat opvalt is dat de domeinen die het best scoren - Organisatie en Bestuur - zijn opgenomen in fase 1 van het Groeipad. Deze fase richt zich op de governance van de organisatie voor het goed inrichten van informatiebeveiliging. De laagst scorende domeinen zijn meer proces- en beheersmatig van aard, waarbij groei in volwassenheid pas later optreedt. We zagen eerder dat deze domeinen binnen de Benchmark MBO ook het laagst scoren.

Onderwijssoort

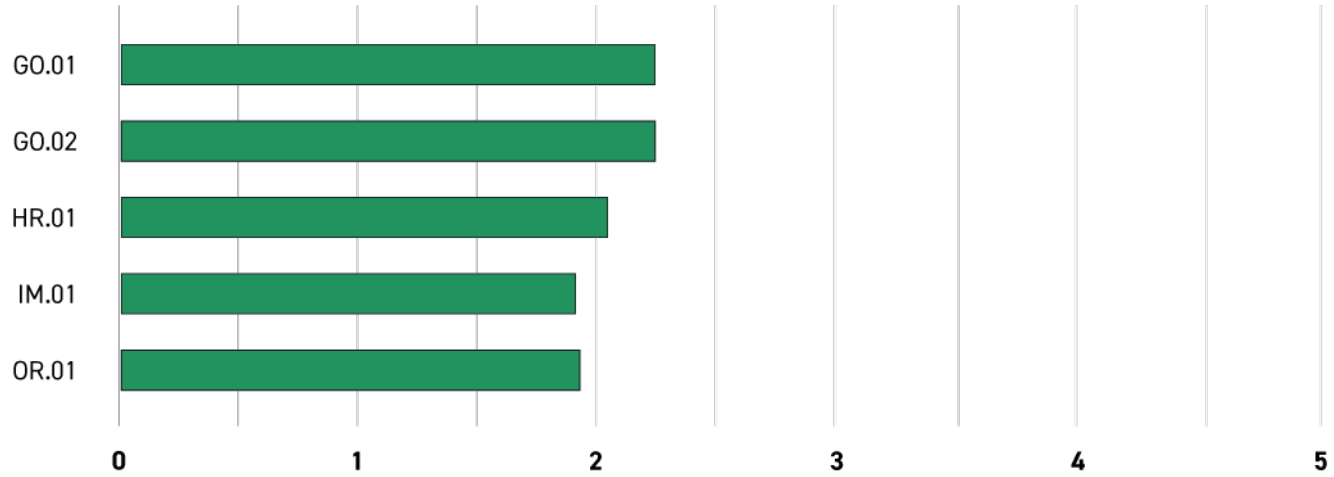
Vergelijken we de resultaten per onderwijssoort dan valt op dat binnen het primair onderwijs vrijwel alle IB-domeinen relatief laag scoren (veel waarden rond 1,1–1,3) en binnen het voortgezet onderwijs juist iets hoger. Door de lage aantallen deelnemers uit het gespecialiseerd onderwijs en samenwerkingsverbanden kan een enkele hoge of lage waarde daar al snel het beeld kleuren.

HOOGST SCORENDE NORMEN

De 5 hoogst scorende normen voor informatiebeveiliging vallen deels binnen de best scorende domeinen organisatie en bestuur:

- **GO.01 Strategie informatiebeveiliging:** de norm die beschrijft dat een schoolbestuur een strategie moet hebben voor informatiebeveiliging.
- **GO.02 Beleid informatiebeveiliging:** de norm die beschrijft dat een schoolbestuur een beleid moet hebben voor informatiebeveiliging.
- **OR.01 Eigenaarschap, rollen, verantwoordelijkheden en aansprakelijkheid:** de norm die beschrijft dat rollen en verantwoordelijkheden belegd moeten worden.
- **IM.01 Incidentmanagement:** de norm die beschrijft dat er een proces moet zijn voor incidenten.
- **HR.01 Werving van medewerkers:** de norm die beschrijft hoe nieuwe medewerkers geworven worden en vereisten stelt voor screening van nieuwe medewerkers.

Grafiek 3 Hoogst scorende normen IB



De normen GO.01 Strategie informatiebeveiliging, GO.02 Beleid informatiebeveiliging en OR.01 Eigenaarschap, rollen, verantwoordelijkheden en aansprakelijkheid zijn randvoorwaardelijk voor het verder implementeren van het normenkader. Voor veel schoolbesturen zijn deze normen dan ook een logisch startpunt van de implementatie. Dit kan verklaren waarom de score gemiddeld hoger is.

De normen IM.01 Incidentmanagement en HR.01 Werving van medewerkers sluiten aan op processen die een schoolbestuur vaak al ingericht heeft. Het werven en screenen van nieuwe medewerkers gebeurt al, onder andere door het gebruik van een VOG. Daarmee is het vaak een kwestie van bestaande processen aanscherpen en formaliseren om tot een hoger volwassenheidsniveau te komen. Dit is voor veel schoolbesturen dan ook makkelijker in te richten dan een compleet nieuw proces. Ook het oplossen van incidenten is niet nieuw voor schoolbesturen en vraagt vooral om aanscherping en formalisering. De 'hogere' score voor IM.01 Incidentmanagement is ook in lijn met de resultaten uit de Monitor Digitalisering Onderwijs 2025. Scholen gaven hierin aan weliswaar een plan te hebben voor incidenten, maar hier nog niet mee geoefend te hebben.

LAAGST SCORENDE NORMEN

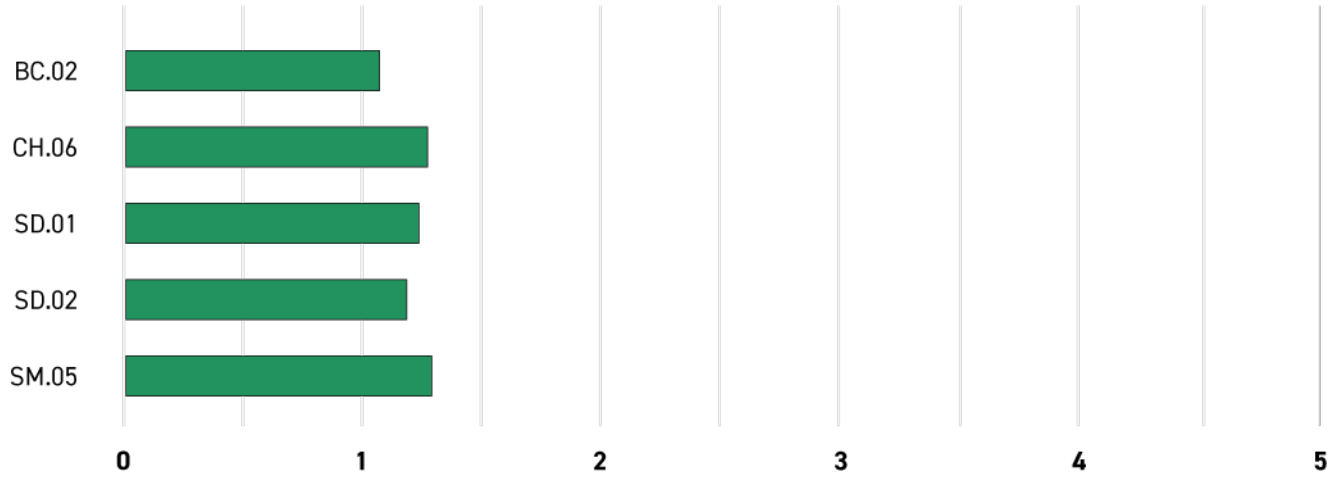
De 5 laagst scorende normen voor informatiebeveiliging komen ook grotendeels voort uit de laagst scorende domeinen:

- **BC.02 Testen van disaster recovery:** de norm die beschrijft dat bedrijfs- en IT-continuïteitsplannen regelmatig getest moeten worden.
- **SD.02 Toegang productieomgeving door ontwikkelaars:** de norm die beschrijft hoe verantwoordelijkheden bij de toegang tot de productie-, test- en ontwikkel-omgeving gescheiden moeten worden.
- **SD.01 Methodiek veilige softwareontwikkeling en -implementatie:** de norm die beschrijft dat er een methodiek voor veilige softwareontwikkeling gebruikt moet worden.
- **CH.06 Overzetten naar productieomgeving:** de norm die beschrijft hoe wijzigingen doorgevoerd moeten worden in de productieomgeving.
- **SM.05 Testen, inspectie en toezicht beveiliging:** de norm die beschrijft hoe de IT-beveiliging wordt getest en gemonitord.

De normen SD.01 Methodiek veilige softwareontwikkeling en -implementatie en SD.02 Toegang productieomgeving door ontwikkelaars zijn voor veel scholen niet van toepassing, omdat ze zelf geen software ontwikkelen. In dat geval zal dit vooral bij de leverancier belegd worden. De norm CH.06 Overzetten naar productieomgeving hangt ook samen met de ontwikkeling van software en is voor veel schoolbesturen complex om in te vullen of niet van toepassing, omdat ze zelf geen software ontwikkelen.

De lage score op norm BC.02 Testen van disaster recovery en norm SM.05 Testen, inspectie en toezicht beveiliging is niet onverwacht. Schoolbesturen zijn veelal nog bezig met het inrichten van maatregelen en dus nog niet klaar om deze structureel te testen.

Grafiek 4 Laagst scorende normen IB



5. Resultaten privacy

Het onderdeel privacy uit het Normenkader IBP is kleiner dan het onderdeel informatiebeveiliging. Het bestaat uit 7 domeinen en 25 normen. We beschrijven hier de resultaten voor privacy.

HOOGST SCORENDE DOMEINEN

De best scorende domeinen binnen het onderdeel privacy zijn:

- Organisatorische inbedding (2,3)
- Beleid (2,2)

We gaan hieronder in op specifieke bevindingen bij deze domeinen.

Domein Organisatorische inbedding

Het domein Organisatorische inbedding is het best scorende domein binnen privacy, hoewel ook dit domein met een score van 2,3 onder volwassenheidsniveau 3 blijft. In de praktijk betekent dit het volgende:

- De belangrijkste rollen en structuren zijn aanwezig, maar nog niet volledig formeel zijn vastgelegd of geborgd. Schoolbesturen zijn bewust bezig met privacy, maar leunen nog sterk op enkele functionarissen.
- De processen zijn vermoedelijk deels informeel en nog niet organisatiebreed of structureel ingericht.
- De functie van functionaris gegevensbescherming is bekend en deels ingericht, maar niet overal optimaal gepositioneerd. Mogelijk staat de onafhankelijkheid en slagkracht van de functionaris gegevensbescherming onder druk en is privacytoezicht wel aanwezig, maar nog niet volledig professioneel ingebed.
- Er is een functionerende kern van privacy-expertise binnen besturen. Privacy is geen ‘blinde vlek’ meer. Er is capaciteit aanwezig, maar samenwerking tussen privacy en informatiebeveiliging is nog niet structureel geïntegreerd.
- Privacy is mogelijk nog onvoldoende vast onderdeel is van de governance van de organisatie, waaronder medezeggenschap.
- Opleiding en training om bewustwording te stimuleren zijn nog niet programmatisch en structureel ingericht. Het privacybewustzijn onstaat mogelijk vooral door incidenten en komt niet voort uit preventief beleid.

Domein Beleid

Het domein Beleid behoort, samen met Organisatorische Inbedding, tot de best scorende domeinen voor privacy, met een score van 2,2. In de praktijk betekent dit het volgende:

- De meeste schoolbesturen hebben een privacybeleid opgesteld, maar dat is vaak nog niet volledig actueel of formeel vastgesteld. Mogelijk is het beleid niet organisatiebreed bekend of geborgd en in de praktijk afhankelijk van enkele sleutelfiguren als een functionaris gegevensbescherming of een privacy officer. De relatief hoge score van het domein Beleid lijkt erop te duiden dat de sector inhoudelijk wel goed bekend is met de AVG-verplichtingen.
- Rollen zijn vaak gedeeltelijk of informeel belegd. De verantwoordelijkheid voor privacy leunt sterk op een centrale privacyfunctionaris. De sector beweegt richting professionalisering, maar een volwassen privacyorganisatie - met onder andere duidelijk belegde rollen en verantwoordelijkheden, overlegstructuren en laagdrempelige manieren om privacygerelateerde vragen te stellen voor medewerkers - bestaat waarschijnlijk nog niet overal.
- Er is aandacht is voor verwerkingen van persoonsgegevens met hoge risico's en DPIA's worden mogelijk wel uitgevoerd, maar niet altijd via een volledig formeel proces. Risicomanagement is vooral reactief of gericht op uitzonderingen. Risicobeheersing is dus wel aanwezig, maar nog niet volledig systematisch ingericht.

LAAGST SCORENDE DOMEINEN

Daar waar het eenvoudig is om de best scorende domeinen aan te wijzen, is dat voor de laagst scorende domeinen minder gemakkelijk. Alle domeinen scoren gemiddeld rond de 1,8. Dat betekent dat geen enkel domein in de buurt komt van volwassenheidsniveau 3.

Algemene bevindingen privacy

De best scorende domeinen binnen privacy - beleid en organisatorische inbedding -zitten allemaal in fase 1 van het Groeipad. Deze fase is gericht op inrichting en governance van de organisatie voor het goed inrichten van je privacy-organisatie. Vrijwel alle andere privacydomeinen hebben eenzelfde score.

Onderwijssoorten

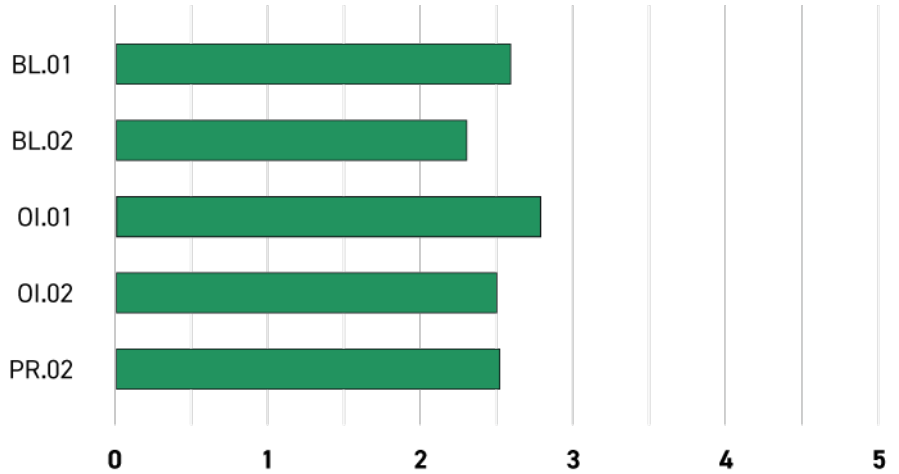
Voor privacy geldt dat het VO in bijna alle domeinen hoger scoort dan het PO, samenwerkingsverbanden en GO. Alleen bij het domein Beleid is het verschil juist klein (0,06). Het gemengd onderwijs scoort op de domeinen Samenwerking en Rechten van betrokkenen iets beter dan het VO.
De domeinen en Beveiliging laten de grootste verschillen zien tussen de onderwijssoorten. Zo scoort binnen Samenwerking het PO een 1,2 en het GO een 1,9. Binnen het domein Beveiliging scoort het PO een 1,2 en het VO een 1,9. Binnen het PO zijn de grootste verschillen in domeinen te zien.
Het domein Samenwerking scoort een 1,2 terwijl Beleid een 2,2 scoort.
Ook hier geldt dat we voorzichtig moeten zijn met het interpreteren van resultaten door lage aantallen deelnemers van samenwerkingsverbanden en van besturen waar alleen de onderwijssoorten gespecialiseerd onderwijs of speciaal basisonderwijs onder vallen.

HOOGST SCORENDE NORMEN

De 5 hoogst scorende normen voor privacy komen net als bij informatiebeveiliging deels overeen met de best scorende domeinen:

- **BL.01 Privacybeleid:** de norm die beschrijft dat een organisatie een privacybeleid heeft vastgesteld.
- **BL.02 Rollen, taken en verantwoordelijkheden:** de norm die beschrijft dat rollen, taken en verantwoordelijkheden met betrekking tot privacy zijn benoemd, belegd en vastgelegd in het privacybeleid.
- **OI.01 Aanwijzing en positie functionaris gegevensbescherming:** de norm die beschrijft dat elke organisatie een functionaris gegevensbescherming (FG) heeft aangesteld en zodanig onafhankelijk heeft gepositioneerd dat deze effectief toezicht kan houden.
- **OI.02 Privacyorganisatie:** de norm die beschrijft dat er naast de FG ruime (juridische) kennis en ervaring binnen de organisatie beschikbaar is over bescherming van persoonsgegevens en relevante wet- en regelgeving.
- **PR.02 Verwerkingsregister opzet en vastlegging verwerkingen:** de norm die beschrijft dat elke organisatie een verwerkingsregister bij houdt dat voldoet aan de wettelijke eisen.

Grafiek 5 Hoogst scorende normen privacy



Bovenstaande normen zijn randvoorwaardelijk voor het verder implementeren van het normenkader. Ze zijn dan ook een logisch startpunt voor die implementatie. Daarnaast zijn bijvoorbeeld het aanstellen van een functionaris gegevensbescherming en het beheren van een verwerkingsregister verplichtingen die volgen uit de AVG waar scholen ook voor de komst van het Normenkader IBP al aan moesten voldoen.

LAAGST SCORENDE NORMEN

De laagst scorende normen vallen binnen de domeinen die eveneens het laagst scoren:

- **GB.03 Beveiliging persoonsgegevens:** De norm die beschrijft dat een organisatie passende technische en organisatorische maatregelen neemt om persoonsgegevens te beveiligen.
- **RB.04 Geautomatiseerde besluitvorming en/of profilering:** De norm die beschrijft dat een organisatie voldoet aan de wettelijke vereisten voor geautomatiseerde individuele besluitvorming, waaronder profilering.
- **PR.06 Gegevensbescherming door privacy by design en privacy by default:** De norm die beschrijft dat een organisatie bij ontwikkeling, selectie en gebruik van toepassingen zo vroeg mogelijk privacybeginselen en -risico's meeneemt, privacy by design en by default toepast en systemen standaard privacyvriendelijk instelt.
- **PR.01Operationele processen:** De norm die beschrijft dat een organisatie de operationele processen waarin persoonsgegevens worden verwerkt in beeld heeft en beschreven.
- **PR.05 DPIA's:** De norm die beschrijft dat een organisatie bij verwerkingen met een hoog risico voor betrokkenen een AVG-conforme DPIA uitvoert en dat de organisatie de uitkomsten daarvan systematisch beheert.

De lage score voor GB.03 Beveiliging persoonsgegevens kan mogelijk verklaard worden door het feit dat een schoolbestuur alleen aan een passend beveiligingsniveau kan voldoen als aan de normen voor informatiebeveiliging wordt voldaan. Zijn die scores laag? Dan werkt dat door in de normen onder privacy die hier betrekking op hebben. Zo zie je binnen het domein Beveiliging een duidelijk verschil tussen de relatief hoge score van GB.01 Datalekken detectie, classificatie en afhandeling (2,2) en de relatief lage score van GB.03 Beveiliging persoonsgegevens (1,2). Dit kan mogelijk verklaard worden doordat het volwassenheidsniveau van informatiebeveiliging over het algemeen lager is en het beveiligen van persoonsgegevens het nodige vraagt van informatiebeveiliging.

Het lijkt er ook op dat het voor scholen makkelijker is om administratieve maatregelen te nemen dan risicogestuurde en preventieve maatregelen. Zo scoort de norm PR.03 Verwerkingsregister actualisatie binnen het domein Processen met een 2,4 relatief hoog, terwijl normen die betrekking hebben op complexe AVG-verplichtingen als profilering, privacy by design en DPIA's duidelijk achterblijven in volwassenheid. Deze normen vragen gespecialiseerde (technische) kennis en inhoudelijke expertise. Juist in organisaties waar privacy als neventaak wordt belegd of waar deze expertise ontbreekt, kan dit voor problemen zorgen.

De RB.04 Geautomatiseerde besluitvorming en/of profilering is met een 1,2 een van de laagst scorende. De lage score kan mogelijk worden verklaard doordat schoolbesturen wellicht onvoldoende hebben geïnventariseerd binnen welke systemen of toepassingen sprake is van geautomatiseerde besluitvorming of profilering, waardoor dit niet als zodanig wordt herkend.

De normen binnen het domein Samenwerking scoren tussen de 1,7 en 1,9. Dit duidt erop dat de normen die daaronder vallen - zoals SW.01 AVG-rollen, SW.02 Toetsing gegevensverstrekking aan derden en SW.03 Doorgifte buiten de EER - nog onvoldoende zijn uitgewerkt. Omdat er in het onderwijs veel met leveranciers wordt gewerkt is dit niet zonder risico. Deze normen hebben namelijk betrekking op het verstrekken aan en verwerken van persoonsgegevens door derden.

6. Conclusies en aanbevelingen

De resultaten van deze verkenning laten zien dat de volwassenheid van schoolbesturen op het gebied van informatiebeveiliging en privacy op alle domeinen nog onvoldoende is. Tegelijkertijd scoren de domeinen en normen die randvoorwaardelijk zijn voor het inrichten van informatiebeveiliging en privacy relatief beter. Dit biedt een solide basis voor verdere ontwikkeling.

OP ORDE BRENGEN VAN DE BASIS

De gemiddelde volwassenheid op het gebied van zowel privacy als informatiebeveiliging binnen het funderend onderwijs bevindt zich nog onder volwassenheidsniveau 3. Dit duidt erop dat structurele elementen weliswaar aanwezig zijn, maar verdere concretisering, implementatie en borging nog ontbreken. Het is een beeld dat aansluit bij het meest recente sectorbeeld van de Autoriteit Persoonsgegevens[15], waarin wordt gesteld dat de onderwijssector “de goede kant opgaat”, maar dat het “op orde brengen van de basis” nog nadrukkelijk om aandacht vraagt.

ONDERSTEUNING

Het programma DVO gaat de mogelijkheid onderzoeken om hulpmiddelen te ontwikkelen die scholen helpen bij het implementeren van normen waar zij nu onvoldoende op scoren. Daarbij wordt ook rekening gehouden met toekomstige ontwikkelingen. Blijft de groei in volwassenheid bij sommige domeinen achter? Dan zal daar extra aandacht aan worden besteed.

15 https://autoriteitpersoonsgegevens.nl/documenten/sectorbeeld-onderwijs-2021-2023

Bijlage A | Volwassenheidsniveaus

Hieronder vind je een toelichting op alle volwassenheidsniveaus[16] van het Normenkader IBP.

Bijlage Volwassenheidsniveau IBP Normenkader

Niveau		Toelichting
1	**Ad hoc**	Er is geen gestructureerde aanpak voor informatiebeveiliging en privacy. Documentatie ontbreekt grotendeels en problemen worden vooral achteraf opgelost. De organisatie is kwetsbaar en de kans op het niet naleven van wet- en regelgeving is groot.
2	**Herhaalbaar**	Er zijn basismaatregelen genomen om risico's te beperken. Er is enige bescherming tegen digitale dreigingen en privacyrisico's, maar procedures worden nog niet altijd formeel en consistent toegepast.
3	**Bepaald**	Procedures en richtlijnen zijn vastgelegd en worden consequent uitgevoerd. Het bestuur kan aantonen dat maatregelen zijn ingevoerd, getest en effectief zijn. De kans op incidenten is hierdoor duidelijk kleiner.
4	**Beheerst**	Beveiligings- en privacymaatregelen worden actief gemonitord en regelmatig geëvalueerd, zowel intern als extern. Beleid en processen worden continu verbeterd en aangepast aan nieuwe wet- en regelgeving. De maatregelen uit niveau 4 bouwen voort op niveau 3.
5	**Continu verbeteren**	Informatiebeveiliging en privacy zijn volledig geïntegreerd in de strategie en dagelijkse praktijk van de organisatie. Het bestuur werkt proactief en vernieuwend aan verdere verbetering. De maatregelen uit niveau 5 bouwen voort op niveau 3 en 4.

16 Opzet en inhoud | Normenkader IBP

Colofon

IBP IN BEELD

Datum van uitgave
Maart 2026

Totstandkoming
Deze verkenning is tot stand gekomen in opdracht van het programma DVO, dankzij een samenwerking tussen Kennisnet, SIVON en GRC-tool leveranciers.

Vormgeving
Van Hulzen Communicatie

Over programma Digitaal Veilig Onderwijs
Met het programma Digitaal Veilig Onderwijs bundelen het ministerie van OCW, Kennisnet, SIVON, de PO-Raad en de VO-raad hun krachten voor een onderwijssector waarin iedere leerling digitaal veilig kan leren en medewerkers digitaal veilig kunnen werken. Het programma biedt schoolbesturen heldere leidraden en een concreet ondersteuningsaanbod. Het programma stimuleert ook dat leveranciers hun productportfolio in lijn brengen met het Normenkader IBP. Zo kunnen scholen voldoen aan hun verantwoordelijkheid om een digitaal veilige organisatie te realiseren. Stap voor stap, Bit by Bit.

Bit by Bit
Samen voor digitaal veilig onderwijs

info@digitaalveiligonderwijs.nl | www.digitaalveiligonderwijs.nl