

94 normen, één maat?

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

Deel A - Informatiebeveiliging

IB 1. Governance

Norm	Categorie	Voorgesteld adaptief niveau	Beknopte onderbouwing en voorwaarden
GO.01	Strategie	3	Een korte, bestuurlijk vastgestelde IBP-strategie geeft richting aan prioriteiten, risicobereidheid en middelen. Ook een éénpitter moet keuzes kunnen uitleggen en periodiek herijken.
GO.02	Beleid	3	Een vastgesteld en gecommuniceerd beleid voorkomt persoonsafhankelijkheid. Een compact kernbeleid met praktische kwaliteitskaarten is voor een éénpitter voldoende.
GO.03	Planning / Roadmap	3	Beperkte capaciteit vraagt juist om prioritering. Een eenvoudige roadmap met maatregelen, eigenaarschap, planning en voortgang is passend.
GO.04	Architectuur	2	Een actueel overzicht van systemen, kernapplicaties, gegevensstromen en afhankelijkheden is nodig. Een eenvoudige baseline-architectuur kan volstaan; een volledig IST/SOLL-model is niet altijd proportioneel.
GO.05	Onafhankelijke toetsing	2*	Periodieke onafhankelijke toetsing blijft nodig, maar kan extern en risicogericht worden ingericht. Een aparte auditcommissie en uitgebreide auditcyclus zijn voor een éénpitter niet noodzakelijk.

IB 2. Organisatie

Norm	Categorie	Voorgesteld adaptief niveau	Beknopte onderbouwing en voorwaarden
OR.01	Eigenaarschap, rollen, verantwoording en verantwoordelijkheid	3	Leg vast wie bestuurlijk verantwoordelijk is, risico's accepteert en eigenaar is van processen, systemen en maatregelen. Rollen mogen worden gecombineerd; verantwoordelijkheden niet.
OR.02	Functiescheiding	2	Volledige functiescheiding is bij weinig medewerkers niet altijd haalbaar. Compenseer rolvermenging met vier-ogencontrole, logging, externe controle of functiescheiding met leveranciers.

IB 3. Risicobeheer

Norm	Categorie	Voorgesteld adaptief niveau	Beknopte onderbouwing en voorwaarden
RM.01	Informatierisicomanagementkader	3	Een vastgesteld risicokader is noodzakelijk om risico's, risicobereidheid, eigenaarschap en eventuele lagere volwassenheidsniveaus aantoonbaar te onderbouwen.
RM.02	Risicobeoordeling	3	Beoordeel risico's herhaalbaar op kans, impact en bestaande maatregelen en herhaal dit periodiek en bij relevante veranderingen. Een eenvoudige methodiek volstaat.
RM.03	Plan voor behandeling en beperking van risico's (inclusief risicoacceptatie)	3	Leg maatregelen, eigenaar, termijn en restrisico vast. Afwijkingen of risicoacceptatie vragen een expliciet besluit, motivering en periodieke herbeoordeling.

IB 4. Personeelsbeheer

Norm	Categorie	Voorgesteld adaptief niveau	Beknopte onderbouwing en voorwaarden
HR.01	Werving	3	Neem screening, betrouwbaarheid en beveiligingsafspraken op in de instroomprocedure. Een korte checklist is voldoende, maar uitvoering moet aantoonbaar zijn.
HR.02	Certificering, training en scholing	2	Gerichte scholing voor relevante rollen is nodig. Een uniform proces voor periodieke toetsing en certificering van alle competenties kan bij een klein team achterwege blijven.
HR.03	Afhankelijkheid van individuen	2	Breng sleutelrollen in beeld en regel achtervang, overdracht en toegang tot noodzakelijke instructies. Volledige functieroulatie en uitgebreide opvolgingsprogramma's zijn niet nodig.
HR.04	Verandering of beëindiging van functie	3	Gebruik een vaste in-, door- en uitstroomwerkwijze voor rechten, middelen, kennis en verantwoordelijkheden. Een korte checklist met controle op uitvoering volstaat.
HR.05	Kennisdeling	2	Algemene kennis kan informeel worden gedeeld. Kritieke werkinstructies, herstellkennis en vervangingsafspraken moeten wel aantoonbaar beschikbaar zijn.
HR.06	Veiligheidsbewustzijn	3	Organiseer terugkerende bewustwording over onder meer phishing, veilig delen, incidentmeldingen en persoonsgegevens. Het programma mag compact zijn, maar niet incidenteel.

IB 5. Configuratiebeheer

Norm	Categorie	Voorgesteld adaptief niveau	Beknopte onderbouwing en voorwaarden
CO.01	Identificatie en onderhoud van configuratie-items	2	Houd apparatuur, applicaties, kernsystemen, eigenaarschap en leveranciers via een eenvoudige vaste werkwijze inzichtelijk. Volledig geformaliseerd configuratiebeheer is niet nodig, maar kritieke middelen mogen niet buiten beeld raken.
CO.02	Configuratiegegevens en baseline	2 afhankelijk van toepasselijkheid	Een overzicht van applicaties, belangrijke configuraties, koppelingen en leveranciers kan volstaan. Technische configuratiebaselines mogen bij de leverancier liggen, mits de school relevante instellingen en afhankelijkheden kent.

IB 6. Incident/probleembeheer

Norm	Categorie	Voorgesteld adaptief niveau	Beknopte onderbouwing en voorwaarden
IM.01	Incidentmanagement	3	Zorg voor een herkenbare meldroute, registratie, beoordeling en opvolging van incidenten. De servicedesk van een leverancier kan hiervoor worden ingezet.
IM.02	Incident escalatie	2	Een eenvoudige escalatieroute met bekende contactpersonen en urgentiecriteria volstaat. Voor cyberincidenten, datalekken en ernstige uitval gelden vooraf vastgelegde escalatieafspraken.
IM.03	Incidentrespons op (cyber) beveiligingsincidenten	3	Leg rollen, bereikbaarheid, bevoegdheden, communicatie en herstelkeuzes vooraf vast. Een compact incidentresponsplan met contactkaart is passend.
IM.04	Probleembeheer	2 afhankelijk van uitvoering	Terugkerende problemen moeten worden herkend, geëscaleerd en gevolgd tot structurele oplossing. Technische root-cause analyse kan bij de ICT- of applicatieleverancier liggen.

IB 7. Wijzigingsbeheer

Norm	Categorie	Voorgesteld adaptief niveau	Beknopte onderbouwing en voorwaarden
CH.01	Normen en procedures voor aanpassingen	2	Beoordeel en autoriseer significante wijzigingen vooraf en leg uitvoering en terugval vast. Routinewijzigingen mogen eenvoudiger worden behandeld.
CH.02	Impact assessment, prioriteren en autoriseren	2	Laat eigenaar en beheerpartner gevolgen en prioriteit beoordelen. Significante wijzigingen vragen navolgbare goedkeuring; een zware uniforme besluitvormingsstructuur is niet nodig.
CH.03	Noodaanpassingen	2 afhankelijk van toepasseljkheid	Noodwijzigingen moeten worden vastgelegd en achteraf beoordeeld. Technische emergency changes kunnen bij de leverancier liggen, mits de school relevante wijzigingen kan volgen.
CH.04	Testomgeving	2 afhankelijk van toepasseljkheid	Een permanente testomgeving is niet altijd nodig. Voor eigen configuraties, autorisaties, workflows of koppelingen moet wel vooraf worden bepaald hoe veilig wordt getest of gevalideerd.
CH.05	Testen van aanpassingen	2 afhankelijk van toepasseljkheid	Voor eigen wijzigingen volstaat een eenvoudige, herhaalbare testwerkwijze. Technische tests kunnen bij de leverancier liggen, mits school-specifieke wijzigingen waar nodig afzonderlijk worden gevalideerd.
CH.06	Promotie naar productie	2 afhankelijk van toepasseljkheid	Technische release kan bij de leverancier liggen. Voor wijzigingen in eigen configuraties, autorisaties, workflows of koppelingen blijft voorafgaande acceptatie door de school nodig.

IB 8. Systeemontwikkeling

Norm	Categorie	Voorgesteld adaptief niveau	Beknopte onderbouwing en voorwaarden
SD.01	Methodiek voor veilige softwareontwikkeling en -implementatie	2*	Bij een éénpitter zonder eigen softwareontwikkeling richt deze norm zich op veilige aanschaf en implementatie van applicaties. Beveiliging, privacy, continuïteit, koppelingen en eigenaarschap worden vooraf beoordeeld; ontwikkelspecifieke processen liggen bij de leverancier.
SD.02	Toegang tot de productieomgeving door ontwikkelaars	Nvt / leverancier	Bij uitsluitend standaardapplicaties is deze norm voor de eigen uitvoering niet van toepassing; de beheersing ligt bij de leverancier. Bij eigen ontwikkeling of schoolgebonden maatwerk geldt niveau 3 als uitgangspunt.
SD.03	Data conversie en/of migratie	2	Voor eenvoudige migraties kan beperkte validatie volstaan. Migraties van leerling-, personeels- of financiële kerngegevens vragen aantoonbare controle en niveau 3.

IB 9. Gegevensbeheer

Norm	Categorie	Voorgesteld adaptief niveau	Beknopte onderbouwing en voorwaarden
DM.01	Data (en systeem) eigenaarschap	3	Wijs eigenaren aan voor gegevens en systemen en leg bevoegdheden vast voor toegang, gebruik, bewaren, uitwisseling en verwijdering.
DM.02	Classificatie	3	Gebruik een eenvoudig classificatiemodel met praktische behandelingsregels. Medewerkers moeten weten welke informatie extra bescherming vraagt.
DM.03	Beveiligingseisen voor gegevensbeheer	3	Leg vast hoe gevoelige gegevens worden beschermd tegen ongeoorloofde toegang, onjuiste verwerking en onveilige uitwisseling.
DM.04	Inrichting van opslag en retentie	3	Wijs toegestane opslaglocaties aan en stel bewaartermijnen en verantwoordelijkheden vast. Dit geldt ook voor gegevens in kernapplicaties.
DM.05	Uitwisseling van (gevoelige) gegevens	3	Leg regels vast voor ontvangers, kanalen, toegang en beveiliging bij gegevensuitwisseling. Pas maatregelen aan op de vertrouwelijkheid van de gegevens.
DM.06	Verwijderen van data	3	Leg veilige verwijdering en vernietiging vast voor digitale en papieren gegevens, inclusief uitvoering en controle.

IB 10. Identiteits- en toegangsbeheer

Norm	Categorie	Voorgesteld adaptief niveau	Beknopte onderbouwing en voorwaarden
ID.01	Toegangsrechten	3	Bepaal toegang op basis van rol, taak en noodzaak. Een eenvoudige autorisatiematrix voor kernapplicaties en technische voorzieningen is passend.
ID.02	Administratie van toegangsrechten	2	Accounts en rechten moeten tijdig worden aangepast, maar volledige functiescheiding tussen aanvragen, goedkeuren en uitvoeren is niet altijd haalbaar. Compenseer met nacontrole.
ID.03	Super Users	3	Beheerdersrechten vragen expliciete goedkeuring, beperking, aparte accounts en controle. Dit geldt ook voor beheeraccounts binnen kernapplicaties.
ID.04	Noodtoegang (envelopprocedure/breek-het-glasprocedure)	3	Regel wie noodtoegang mag gebruiken, hoe deze wordt geactiveerd en hoe gebruik achteraf wordt gecontroleerd. Een korte procedure volstaat.
ID.05	Periodieke beoordeling van toegangsrechten	3	Beoordeel periodiek of accounts en rechten nog nodig zijn. Richt de frequentie risicogestuurd in en leg afwijkingen en herstel vast.

IB 11. Beveiligingsbeheer

Norm	Categorie	Voorgesteld adaptief niveau	Beknopte onderbouwing en voorwaarden
SM.01	Security baselines	3	Leg minimale beveiligingsinstellingen vast voor apparatuur, infrastructuur én kernapplicaties. Leveranciers-baselines kunnen worden gebruikt als ze aansluiten op risico en gebruik.
SM.02	Authenticatiemechanismen	3	Gebruik sterke authenticatie voor gebruikers, beheerders en kernapplicaties. Zwakke of gedeelde toegang tot gevoelige gegevens is niet passend.
SM.03	Mobiele apparaten en telewerken	3	Stel regels vast voor mobiel werken en voer passende maatregelen uit, zoals apparaatbeheer, versleuteling en toegangsbeveiliging.
SM.04	Logging	3	Bepaal risicogericht welke gebeurtenissen worden gelogd en opgevolgd. Neem ook relevante beheer- en gebruikershandelingen in kritieke kernapplicaties mee.
SM.05	Testen van, inspectie van en toezicht op beveiliging	2	Voer risicogerichte controles en scans uit. Een vast programma van penetratie- en social-engineeringtests is niet altijd proportioneel, maar bevindingen moeten worden opgevolgd.
SM.06	Patchbeheer	3	Houd software en apparatuur ondersteund en herstel kwetsbaarheden binnen passende termijnen. De uitvoering kan bij de leverancier liggen en verhuist dan naar leveranciersmanagement; de school controleert periodiek de uitvoering.
SM.07	Beheer van bedreigingen en kwetsbaarheden	3	Zorg dat relevante kwetsbaarheden en bedreigingen worden gesignaleerd en opgevolgd. Uitvoering kan bij leveranciers liggen; de school bewaakt dat relevante risico's aantoonbaar worden behandeld.
SM.08	Beschikbaarheid en bescherming van infrastructuur	2 afhankelijk van toepasseljkheid	Technische bescherming en beschikbaarheidsbewaking kunnen grotendeels bij leveranciers liggen. De school stelt eisen en bewaakt of kritieke voorzieningen passend zijn beschermd.
SM.09	Onderhoud van de infrastructuur	2 afhankelijk van toepasseljkheid	Onderhoud, lifecycle en vervanging kunnen bij de beheerleverancier liggen. Voor lokaal beheerde voorzieningen blijft een eenvoudige eigen werkwijze nodig.
SM.10	Beheer van cryptografische sleutels	2 afhankelijk van toepasseljkheid	Sleutelbeheer ligt vaak bij cloud- en applicatieleveranciers. Eigen certificaten, sleutels en secrets moeten wel aantoonbaar worden beheerd.
SM.11	Network security	3	Beveilig netwerkverbindingen, wifi en beheer en pas segmentatie toe waar het risico dit vraagt. Technische uitvoering kan via leveranciersmanagement worden belegd, met periodieke controle door de school.
SM.12	Beheersing van malware-aanvallen	3	Zorg voor actuele bescherming tegen malware op apparaten, e-mail en andere relevante toegangspunten. Uitvoering kan bij de leverancier liggen; de school controleert dat de maatregel structureel werkt.

Norm	Categorie	Voorgesteld adaptief niveau	Beknopte onderbouwing en voorwaarden
SM.13	Bescherming van beveiligingstechnologie	3	Beperk beheer van beveiligingsvoorzieningen tot bevoegde personen en controleer wijzigingen. Ook uitbesteede beveiligingstechnologie moet aantoonbaar beschermd zijn.

IB 12. Fysieke beveiliging

Norm	Categorie	Voorgesteld adaptief niveau	Beknopte onderbouwing en voorwaarden
PH.01	Fysieke beveiligingsmaatregelen	2	Beveilig gebouwen, apparatuur en gevoelige dossiers passend. Een volledig formeel pakket van bouwkundige en omgevingsmaatregelen is niet altijd nodig.
PH.02	Beheer van fysieke toegangsrechten	2	Houd toegang tot kritieke ruimten en sleutels beheersbaar. Volledige toegangsregistratie voor iedere technische ruimte is bij eenvoudige locaties niet altijd proportioneel.

IB 13. IT-operatie

Norm	Categorie	Voorgesteld adaptief niveau	Beknopte onderbouwing en voorwaarden
OP.01	Job processing	2 afhankelijk van toepasselijkheid	Geautomatiseerde taken, koppelingen en synchronisaties liggen vaak bij applicatie- of ICT-leveranciers. Voor eigen taken is minimaal een eenvoudige werkwijze voor controle en foutopvolging nodig.
OP.02	Procedures voor back-up en herstel	3	De school moet per kritieke applicatie weten welke gegevens worden geback-up, hoe herstel plaatsvindt en binnen welke termijn. Uitvoering kan bij de leverancier liggen, maar herstelbaarheid wordt periodiek gecontroleerd.
OP.03	Capaciteits- en prestatiebeheer	2 afhankelijk van toepasselijkheid	Technische capaciteitsbewaking kan bij leveranciers liggen. De school bewaakt of kritieke applicaties, verbindingen en voorzieningen in de praktijk voldoende beschikbaar en performant blijven.

IB 14. Bedrijfscontinuïteitsbeheer

Norm	Categorie	Voorgesteld adaptief niveau	Beknopte onderbouwing en voorwaarden
BC.01	Bedrijfscontinuïteitsplanning	2	Bepaal kritieke processen, uitvaltolerantie, afhankelijkheden en werkbare alternatieven. Korte continuïteitskaarten kunnen volstaan zonder volledig geïntegreerd bedrijfscontinuïteitsplanning.
BC.02	Testen van Disaster recovery	2	Test kritieke herstelmogelijkheden periodiek en leg verbeterpunten vast. Volledig geïntegreerde end-to-end-tests met alle leveranciers zijn niet altijd proportioneel.
BC.03	Externe back-upopslag	3	Back-up en productie moeten voldoende gescheiden zijn en aantoonbaar herstelbaar blijven. De uitvoering kan bij de leverancier liggen en verhuist dan naar leveranciersmanagement; de school blijft verantwoordelijk voor periodieke controle.
BC.04	Gegevensreplicatie	2 afhankelijk van toepasselijkenheid	Replicatie moet aansluiten op de herstelbehoefte. Als herstel uit externe back-up binnen de BIA-eisen past, hoeft continue replicatie niet te worden ingericht.
BC.05	Crisisbeheer	3	Zorg voor een compact crisisplan met rollen, vervangers, contacten en communicatieafspraken en oefen periodiek een passend scenario.

IB 15. Ketenbeheer

Norm	Categorie	Voorgesteld adaptief niveau	Beknopte onderbouwing en voorwaarden
SC.01	Service level overeenkomst	3	Maak voor kritieke ICT- en applicatiediensten afspraken over beschikbaarheid, beveiliging, herstel, ondersteuning en verantwoordelijkheden.
SC.02	Service level beheer	2	Beoordeel kritieke dienstverlening periodiek en volg afwijkingen op. Een zware uniforme SLA-cyclus voor iedere leverancier is niet nodig.
SC.03	Risicobeheer van leveranciers	3	Beoordeel kritieke ICT- en applicatieleveranciers vooraf op beveiliging, privacy, continuïteit en afhankelijkheid en leg resterende risico's vast.
SC.04	Interne beheersing bij derden	3	Beoordeel de beheersing van kritieke ICT- en applicatieleveranciers periodiek en leg tekortkomingen en opvolging vast. De diepgang wordt afgestemd op het risico; niet iedere leverancier vraagt dezelfde beoordeling.

Deel B - Privacy

P 1. Beleid

Norm	Categorie	Voorgesteld adaptief niveau	Beknopte onderbouwing en voorwaarden
BL.01	Privacybeleid	3	Een actueel, vastgesteld en begrijpelijk privacybeleid vertaalt de privacybeginselen naar de schoolpraktijk. Combineer het met GO.02 en communiceer wijzigingen. Een compact beleid kan volledig zijn; onbekend of niet vastgesteld beleid is geen passende eindtoestand.
BL.02	Rollen, taken en verantwoordelijkheden	3	Benoem en leg vast wie privacybesluiten neemt, maatregelen uitvoert, risico's behandelt en het register bijhoudt. Een kleine rollentabel kan met OR.01 worden gecombineerd. Het bestuur blijft eindverantwoordelijk; de FG adviseert en houdt onafhankelijk toezicht.
BL.03	Risico's verwerking persoonsgegevens	3	Neem privacyrisico's op in het gezamenlijke risicoproces en beoordeel gevolgen voor rechten en vrijheden van betrokkenen. Leg hoge risico's, maatregelen en bevoegde besluitvorming vast. Alleen financiële of operationele schade voor het bestuur beoordelen is onvoldoende.

P 2. Processen

Norm	Categorie	Voorgesteld adaptief niveau	Beknopte onderbouwing en voorwaarden
PR.01	Operationele processen	3	Breng processen waarin persoonsgegevens worden verwerkt in beeld, wijs eigenaren aan en beschrijf ten minste de hoogrisicoprocessen. Een compact procesoverzicht met kwaliteitskaarten is passend. Detail-Voorgesteld adaptief niveau mag verschillen; overzicht en verantwoordelijkheid blijven organisatiebreed geborgd.
PR.02	Verwerkingsregister opzet en vastlegging verwerkingen	3	Houd een register bij met de wettelijk vereiste gegevens en duidelijke AVG-rollen. Maak verwerkingen en bijbehorende privacyafwegingen inzichtelijk, niet alleen gebruikte applicaties. Een sectorsjabloon kan veel werk besparen, maar moet aansluiten op wat de school werkelijk doet.
PR.03	Verwerkingsregister actualisatie	3	Leg vast wie nieuwe en gewijzigde verwerkingen bijwerkt en wanneer volledigheid wordt gecontroleerd. Verbind dit met inkoop en veranderingen in de schoolpraktijk. Een jaarlijkse controle is een bruikbaar vangnet, maar vervangt het direct verwerken van relevante wijzigingen niet.

Norm	Categorie	Voorgesteld adaptief niveau	Beknpte onderbouwing en voorwaarden
PR.04	Identificatie risico's gegevensverwerking met behulp van pre-DPIA's	3	Gebruik een vaste, korte voorbeoordeling om nieuwe en gewijzigde verwerkingen op mogelijke hoge risico's te toetsen. Leg de uitkomst en motivering vast en breng ook bestaande verwerkingen in beeld. Het tijdig herkennen van een DPIA-plicht mag niet van toeval afhangen.
PR.05	DPIA's	3	Voer waar vereist een DPIA uit voordat de verwerking start en volg maatregelen op. Betrek de FG en motiveer afwijkingen van diens advies. Collectieve DPIA's zijn bruikbaar na toetsing aan de eigen inrichting. Een resterend hoog risico kan voorafgaande raadpleging van de AP vereisen en niet simpelweg worden geaccepteerd.
PR.06	Gegevensbescherming door privacy by design en privacy by default	2*	Bij een beperkt, stabiel pakket standaardapplicaties kunnen privacyafwegingen en instellingen per toepassing worden beoordeeld, zonder volledig uitgewerkte organisatiebrede ontwerpbeginselen en richtlijnen.
PR.07	Bewaar- en vernietigingsbeleid	3	Stel bewaartermijnen en verwijderingsafspraken vast en voer deze consequent uit. Combineer beleid en procedures met DM.04 en DM.06. Neem zowel digitale als papieren gegevens mee. De uitvoering moet navolgbaar zijn; een bewaartermijnenlijst zonder verwijdering is onvoldoende.

P 3. Organisatorische inbedding

Norm	Categorie	Voorgesteld adaptief niveau	Beknpte onderbouwing en voorwaarden
OI.01	Aanwijzing en positie functionaris gegevensbescherming	3	Zorg voor een deskundige, onafhankelijke en bereikbare FG met voldoende tijd, middelen en toegang tot het bestuur. Betrek de FG tijdig en borg rechtstreeks advies en verslaglegging. Een externe FG kan volledig passen; onduidelijke positionering of belangenconflicten niet.
OI.02	Privacyorganisatie	2	Een intern aanspreekpunt, toegankelijke deskundige ondersteuning naast de FG en informele afstemming met informatiebeveiliging kunnen voldoende praktisch functioneren. Een afzonderlijk privacyteam met formele overlegcyclus en vastgestelde reactietijden kan bij een klein team achterwege blijven.
OI.03	Betrokkenheid me-dezeggenschap	3	Leg vast wanneer de MR wordt geïnformeerd, geraadpleegd en om instemming wordt gevraagd. Verwerk dit in de bestaande besluitvormingsprocedure. Een éénpitter kan dit compact organiseren; wettelijke me-dezeggenschapsrechten zijn niet afhankelijk van de omvang van het bestuur.

Norm	Categorie	Voorgesteld adaptief niveau	Beknopte onderbouwing en voorwaarden
OI.04	Bewustwording bescherming persoonsgegevens	3	Neem privacy op in introductie, terugkerende instructies en het onderwijs aan leerlingen. Gebruik herkenbare situaties rond foto's, dossiers, delen en rechten. Combineer met HR.06. Een vast programma hoeft niet omvangrijk te zijn, maar incidentele aandacht alleen is onvoldoende.

P 4. Rechten van betrokkenen

Norm	Categorie	Voorgesteld adaptief niveau	Beknopte onderbouwing en voorwaarden
RB.01	Afhandeling rechten van betrokkenen	3	Gebruik een vaste procedure voor ontvangst, identiteitscontrole, beoordeling, termijnen en afhandeling van verzoeken. Leg besluiten vast en zorg dat medewerkers verzoeken herkennen. Ook bij weinig verzoeken moeten leerlingen, ouders en medewerkers hun rechten tijdig en daadwerkelijk kunnen uitoefenen.
RB.02	Informatieplicht	3	Informeer betrokkenen tijdig en begrijpelijk over verwerking van hun gegevens en hun rechten. Houd privacyverklaring, formulieren en relevante cookie-informatie passend en actueel. Een duidelijke standaardtekst helpt, maar moet de werkelijke verwerkingen beschrijven en bij de doelgroep aansluiten.
RB.03	Toestemming	3	Bepaal welke verwerkingen op toestemming berusten. Vraag geldige toestemming, registreer deze consequent en maak intrekking eenvoudig. Voorkom dat toestemming wordt gebruikt waar een andere grondslag geldt. Een klein aantal leerlingen maakt een onduidelijke of niet-aantoonbare toestemming niet passend.
RB.04	Geautomatiseerde besluitvorming en/of profilering	3	Breng gebruik van algoritmen, profilering en geautomatiseerde besluiten in beeld en documenteer dit. Borg informatie, passende menselijke beoordeling, procedures voor betwisting en benodigde DPIA's. Gebruik van standaardleermiddelen sluit profilering niet uit. Zonder relevante toepassingen kunnen uitvoeringsonderdelen gemotiveerd niet van toepassing zijn.

P 5. Samenwerking

Norm	Categorie	Voorgesteld adaptief niveau	Beknopte onderbouwing en voorwaarden
SW.01	AVG-rollen	3	Beoordeel vooraf of een partij verwerker, gezamenlijke of zelfstandige verwerkingsverantwoordelijke is en maak passende afspraken. Beheer deze centraal en houd zicht op subverwerkers. Een verwerkersovereenkomst is niet voor iedere samenwerkingspartner de juiste vorm.
SW.02	Toetsing gegevensverstrekking aan derden	2*	Bij weinig overzichtelijke gegevensstromen kan toetsing zijn ingebed in inkoop, leerlingadministratie en samenwerking, zonder volledig uniform organisatiebreed toetsings- en besluitvormingsproces. Reguliere verstrekkingen zijn beoordeeld; nieuwe of afwijkende verstrekkingen worden vooraf aan een deskundig aanspreekpunt voorgelegd. Leg relevante afwegingen vast.
SW.03	Doorgifte buiten de EER	2	Beoordeel doorgiften vooraf en leg landen, partijen en geldige waarborgen vast in inkoop- en verwerkingsdocumentatie. Bij weinig leveranciers kan een afzonderlijk, volledig uitgewerkt hertoetsingsproces ontbreken.

P 6. Beveiliging

Norm	Categorie	Voorgesteld adaptief niveau	Beknopte onderbouwing en voorwaarden
GB.01	Datalekken detectie, classificatie en afhandeling	3	Zorg voor een toegankelijk meldpunt, vaste beoordeling, registratie, beheersing, herstel en evaluatie van datalekken. Leg rollen en escalatie vast en combineer met incidentmanagement. Een kleine school moet evenzeer snel herkennen wanneer persoonsgegevens zijn geraakt en welke actie nodig is.
GB.02	Melding datalekken	3	Leg vast wie de meldplicht beoordeelt, aan de AP meldt en betrokkenen informeert waar dat vereist is. Borg wettelijke termijnen, vastlegging, conceptberichten en crisiscommunicatie. Afhankelijkheid van een afwezige directeur of leverancier mag tijdige melding niet blokkeren.
GB.03	Beveiliging persoonsgegevens	3	Passende beveiliging moet structureel worden ingericht en aangetoond, in samenhang met het IB-deel. De openbare norm verwijst naar de IB-normen en bevat geen aparte Voorgesteld adaptief niveaubeschrijvingen. De 3 is daarom een eigen doelkeuze in dit adaptieve profiel, geen zelfstandige officiële score. Lagere IB-doelen vragen afzonderlijke beoordeling en bewijzen geen volledige naleving van GB.03.

P 7. Verantwoording

Norm	Categorie	Voorgesteld adaptief niveau	Beknopte onderbouwing en voorwaarden
VW.01	Rapportage naleving AVG	2	Een jaarlijkse terugblik met de FG en een beknopt verslag in de bestaande bestuurs- en jaarverslagcyclus kunnen passend zijn, zonder volledig gedocumenteerd rapportage- en informatieverzamelproces. Leg bevindingen, besluiten en acties vast en informeer relevante interne en externe belanghebbenden.

Toelichting bij 2*: bij deze norm stellen wij een adaptieve invulling voor die op onderdelen kan afwijken van de formele uitwerking van het betreffende volwassenheidsniveau in het huidige Normenkader IBP. De voorgestelde beheersing achten wij voor een kleine schoolorganisatie proportioneel, mits het risico aantoonbaar wordt beheerst en eventuele restrisico's expliciet worden beoordeeld en geaccepteerd.