



Samen
ontdekken
en leren

Beleidsplan IBP

Documentnaam	Beleidsplan IBP	2025-11-04
Auteur	Ricardo Teeuwsen IBP'er	Pagina 1 van 23
Status	Definitief	

Documentgeschiedenis

Revisies

Versie	Datum	Auteur	Review
1.0	2-4-2025	Ricardo Teeuwsen	
2.0	7-7-2025	Ricardo Teeuwsen	
3.0	04-11-2025	Marjolein Wenting	Van concept naar definitief

Vaststelling

Naam	Functie	Versie	Datum
GMR	Voorzitter GMR instemming	2.0	18-09-2025
Directeuren	Ter kennisgeving	3.0	13-11-2025
Marjolein Wenting	Bestuurder Vastgesteld	3.0	

Documentclassificatie

Classificatie	Beschrijving
Openbaar	Dit document mag zonder beperkingen worden gedeeld

Documentnaam	Beleidsplan IBP	2025-11-04
Auteur	Ricardo Teeuwsen IBP'er	Pagina 2 van 23
Status	Definitief	

Inhoud

Begrippenlijst IBP-beleid – Paraat Scholen	5
Inleiding.....	7
Onze intentie.....	7
Doelstelling.....	7
Reikwijdte.....	8
Juridisch kader.....	8
Wettelijke en reglementaire kaders	8
Normen en standaarden	8
Eigenaarschap en verantwoordelijkheden	9
Three Lines model.....	9
Eerste lijn: eindverantwoordelijkheid bij het bestuur.....	9
Tweede lijn: adviseren en ondersteunen.....	9
Derde lijn: onafhankelijke controle.....	10
Medezeggenschap.....	10
Risicomanagement Paraat scholen	10
Kennis en Afhankelijkheid Medewerkers.....	10
Bedrijfscontinuïteit.....	10
Back-up en Herstel.....	11
Fysieke Beveiliging	11
Systeem- en Data-eigenaarschap en Configuratiebeheer	12
Securitybaseline	14
Bewustwording	14
Incident- en Probleemmanagement	14
Risicomanagement Leveranciers	14
Werkplekken en Mobiele Apparaten.....	15
Identiteits- en Toegangsbeheer	15
Vulnerabilitymanagement en Pentesting	15
Patchmanagement.....	15
Logging.....	15
Digitaal Sleutelbeheer.....	15
Uitgangspunten privacy.....	16
Persoonsgegevens.....	16
Privacyvuistregels	16
Beleidsthema's privacy	18

Documentnaam	Beleidsplan IBP	2025-11-04
Auteur	Ricardo Teeuwssen IBP'er	Pagina 3 van 23
Status	Definitief	

Verwerkingsregister.....	18
Legitiem doel en doelbinding	18
Grondslag	19
Informatieplicht	20
Toestemming.....	20
Privacy by design en privacy by default.....	21
Dataminimalisatie	21
Bewaartermijnen	21
Afhandelen van datalekken	21
Data Protection Impact Assessment.....	22
Uitwisseling persoonsgegevens.....	22
Gegevensverwerking buiten de EER.....	22
Rechten van betrokkenen	22
Verantwoording IBP	23
Naleving AVG.....	23
Rapportage	23
Beleidsherziening	23

Documentnaam	Beleidsplan IBP	2025-11-04
Auteur	Ricardo Teeuwsen IBP'er	Pagina 4 van 23
Status	Definitief	

Begrippenlijst IBP-beleid – Paraat Scholen

Begrip	Omschrijving
AVG (Algemene Verordening Gegevensbescherming)	Europese privacywet die regels stelt voor het verwerken van persoonsgegevens. Geldt voor alle organisaties die persoonsgegevens verwerken, inclusief scholen.
UAVG (Uitvoeringswet AVG)	Nederlandse aanvulling op de AVG. Regelt specifieke zaken binnen de AVG die EU-lidstaten zelf mogen invullen, zoals de minimumleeftijd voor toestemming (16 jaar in Nederland), en wie toezicht houdt (de Autoriteit Persoonsgegevens).
BIA (Business Impact Analyse)	Analyse die in kaart brengt welke processen kritiek zijn voor de organisatie en wat de impact is bij verstoring ervan.
BCP (Bedrijfscontinuïteitsplan)	Plan met maatregelen om essentiële processen voort te zetten bij verstoringen, bijvoorbeeld ICT-uitval of crisissituaties.
BIV-classificatie	Beoordeling van systemen op basis van Beschikbaarheid, Integriteit en Vertrouwelijkheid. Bepaalt welke beveiligingsmaatregelen nodig zijn.
CMDB (Configuration Management Database)	Overzicht waarin alle IT-systemen, eigenaars en configuraties zijn vastgelegd.
Datalek	Beveiligingsincident waarbij persoonsgegevens onbedoeld worden blootgesteld, verloren, gewijzigd of verspreid.
DPIA (Data Protection Impact Assessment)	Verplichte risicoanalyse bij verwerkingen met een hoog privacyrisico.
FG (Functionaris voor Gegevensbescherming)	Onafhankelijke toezichthouder binnen de organisatie die toezicht houdt op naleving van de AVG en adviseert over privacy.
IBP (Informatiebeveiliging en Privacy)	Verzamelnaam voor maatregelen en beleid om informatie en persoonsgegevens veilig te beheren.
IAM (Identity and Access Management)	Systeem en beleid voor het beheren van gebruikersidentiteiten en toegangsrechten tot systemen en gegevens.
Incidentmanagement	Proces voor het melden, registreren en oplossen van beveiligings- en privacy-incidenten.

Documentnaam	Beleidsplan IBP	2025-11-04
Auteur	Ricardo Teeuwsen IBP'er	Pagina 5 van 23
Status	Definitief	

Begrip	Omschrijving
Logging	Het vastleggen van gebruikers- en systeemactiviteiten ten behoeve van toezicht, forensisch onderzoek en auditing.
Normenkader IBP	Sectorale standaard voor informatiebeveiliging en privacy in het onderwijs, opgesteld door Kennisnet, SIVON en partners.
Persoonsgegevens	Alle informatie die herleidbaar is tot een individu, zoals naam, leerlingnummer, IP-adres of gezondheidsgegevens.
Privacy by design	Privacy wordt vanaf de start meegenomen in het ontwerp van systemen, processen en werkwijzen.
Privacy by default	Standaardinstellingen in systemen zijn zo privacyvriendelijk mogelijk, tenzij de gebruiker anders kiest.
Proceseigenaar	Degene die verantwoordelijk is voor het functioneren, naleven en verbeteren van een proces.
Securitybaseline	Minimale eisen op het gebied van informatiebeveiliging waar elk systeem aan moet voldoen.
Systeemeigenaar	Verantwoordelijke voor het dagelijks beheer en de beveiliging van een specifiek informatiesysteem.
Toestemming	Vrij gegeven, geïnformeerde en specifieke instemming voor de verwerking van persoonsgegevens. Moet aantoonbaar en herroepbaar zijn.
Verwerkersovereenkomst	Juridisch contract tussen een verwerkingsverantwoordelijke (bijv. schoolbestuur) en een verwerker (bijv. ICT-leverancier) met afspraken over gegevensverwerking.
Verwerkingsregister	Overzicht van alle verwerkingsactiviteiten binnen de organisatie, verplicht volgens de AVG.
Vulnerabilitymanagement	Het opsporen, beoordelen en verhelpen van kwetsbaarheden in systemen om beveiligingsincidenten te voorkomen.

Documentnaam	Beleidsplan IBP	2025-11-04
Auteur	Ricardo Teeuwsen IBP'er	Pagina 6 van 23
Status	Definitief	

Inleiding

Het onderwijs is in toenemende mate afhankelijk van informatie en ICT. Lesmateriaal wordt digitaal aangeboden, toetsingsprogramma's worden digitaal en de resultaten en ontwikkelingen van leerlingen worden opgenomen in een digitaal leerlingvolgsysteem. Daarnaast wordt ook veel gebruikgemaakt van digitale communicatie tussen de school, leerlingen en ouders/verzorgers. Door deze ontwikkelingen neemt het risico op verstoring van het onderwijs, verlies of misbruik van gegevens en overmatige dataverzameling toe. Het is de verantwoordelijkheid van Paraat scholen om dat te voorkomen en een veilige leeromgeving te bieden.

Dit beleid voor informatiebeveiliging en privacy (IBP-beleid) beschrijft hoe Paraat scholen omgaat met de beveiliging van informatie en hoe de verwerking van (persoons)gegevens wordt gewaarborgd en gehandhaafd. In het beleid worden de verschillende rollen en verantwoordelijkheden binnen Paraat scholen op het gebied van informatiebeveiliging en privacy (IBP) beschreven.

Onze intentie

Paraat scholen draagt de verantwoordelijkheid voor het creëren van een veilige werk- en leeromgeving. Dit houdt in dat Paraat scholen passende technische en organisatorische maatregelen toepast om informatie te beschermen en ongeoorloofde toegang, verlies of misbruik te voorkomen.

Het recht op privacy is een grondrecht. Iedereen heeft recht op privacy en bescherming van de persoonlijke levenssfeer. Dit geldt vanzelfsprekend ook voor leerlingen, ouders/verzorgers, onderwijsondersteunend personeel en onderwijzend personeel. Paraat scholen is verantwoordelijkheid voor het waarborgen van de privacy van de leerlingen en het personeel. Dit betekent ook dat deze betrokkenen zeggenschap hebben over het gebruik van hun persoonsgegevens, zoals wettelijk bepaald.

Bij Paraat scholen staat het bieden van goed onderwijs voorop. Om dit te kunnen doen verwerken wij diverse persoonsgegevens van leerlingen, ouders/verzorgers, onderwijsondersteunend personeel en onderwijzend personeel. Paraat scholen vindt het belangrijk om informatie goed te beschermen en veilig en verantwoord met persoonsgegevens om te gaan. Het goed regelen van informatiebeveiliging en privacy in een beleid is noodzakelijk om de gevolgen van mogelijke informatiebeveiliging- en privacyrisico's tot een aanvaardbaar niveau terug te brengen en de voortgang van het onderwijs te kunnen waarborgen.

Doelstelling

Dit IBP-beleid is erop gericht de kwaliteit van de verwerking van (persoons)gegevens en de beveiliging van informatie en systemen binnen Paraat scholen te verhogen. Hierbij moet een juiste balans bestaan tussen veiligheid, privacy en functionaliteit. Het uitgangspunt is dat een veilige werk- en leeromgeving wordt gecreëerd, de privacy van alle betrokkenen wordt gewaarborgd en Paraat scholen voldoet aan relevante wet- en regelgeving. Dit gebeurt onder andere door bewustwording te vergroten over het belang van het zorgvuldig omgaan met informatie, systemen en persoonsgegevens.

Paraat scholen maakt gebruik van het 'Normenkader Informatiebeveiliging en Privacy voor het onderwijs' - oftewel het Normenkader IBP - om inzichtelijk te maken waar de organisatie nu

Documentnaam	Beleidsplan IBP	2025-11-04
Auteur	Ricardo Teeuwssen IBP'er	Pagina 7 van 23
Status	Definitief	

staat en welke maatregelen genomen moeten worden om een veilige werkomgeving te creëren en te voldoen aan de AVG.

Reikwijdte

Dit beleid is van toepassing op alle leerlingen, leerkrachten, medewerkers, bezoekers, ouders/verzorgers, derde partijen en andere gebruikers die toegang hebben tot of werken met de informatie van Paraat scholen. Het beleid heeft betrekking op de verwerking van alle soorten gegevens en informatie waaronder; persoonsgegevens, bedrijfsinformatie en technische gegevens. Het is van toepassing op alle gegevensverwerkingen die onder de AVG vallen.

Informatiebeveiliging en privacy maken integraal onderdeel uit van dit IBP-beleid.

Informatiebeveiliging is een belangrijke voorwaarde voor privacy. Informatiebeveiliging omvat de beveiliging van *alle* informatie, terwijl privacy gaat over de verwerking van persoonsgegevens.

Juridisch kader

Wettelijke en reglementaire kaders

Het juridisch kader voor dit IBP-beleid wordt gevormd door de Algemene Verordening Gegevensbescherming (AVG) en de Uitvoeringswet UAVG. Daarnaast kunnen uit andere wet- en regelgeving verplichtingen of instructies voortvloeien voor de verwerking van persoonsgegevens. Voor Paraat scholen is op dit gebied onder andere de volgende wetgeving van belang:

- Wet op het primair onderwijs
- Wet onderwijstoezicht
- Archiefwet en Archiefbesluit
- Leerplichtwet
- Wet medezeggenschap op scholen
- Arbeidsregelgeving en CAO
- Belastingwetgeving
- Telecommunicatiewet en e-privacy wetgeving

Indien een (mogelijke) strijdigheid tussen dit beleid en de AVG en/of gerelateerde wet- en regelgeving bestaat, dan moet voorafgaand aan een verwerking overlegd worden met de afdeling Juridische zaken en de privacy officer.

Normen en standaarden

Als onderwijssector hebben we afgesproken om toe te werken naar één normenkader om aan de minimale vereisten te voldoen voor digitaal veilig onderwijs. Dit is het 'Normenkader Informatiebeveiliging en Privacy voor het onderwijs'. Dit normenkader beschrijft de regels,

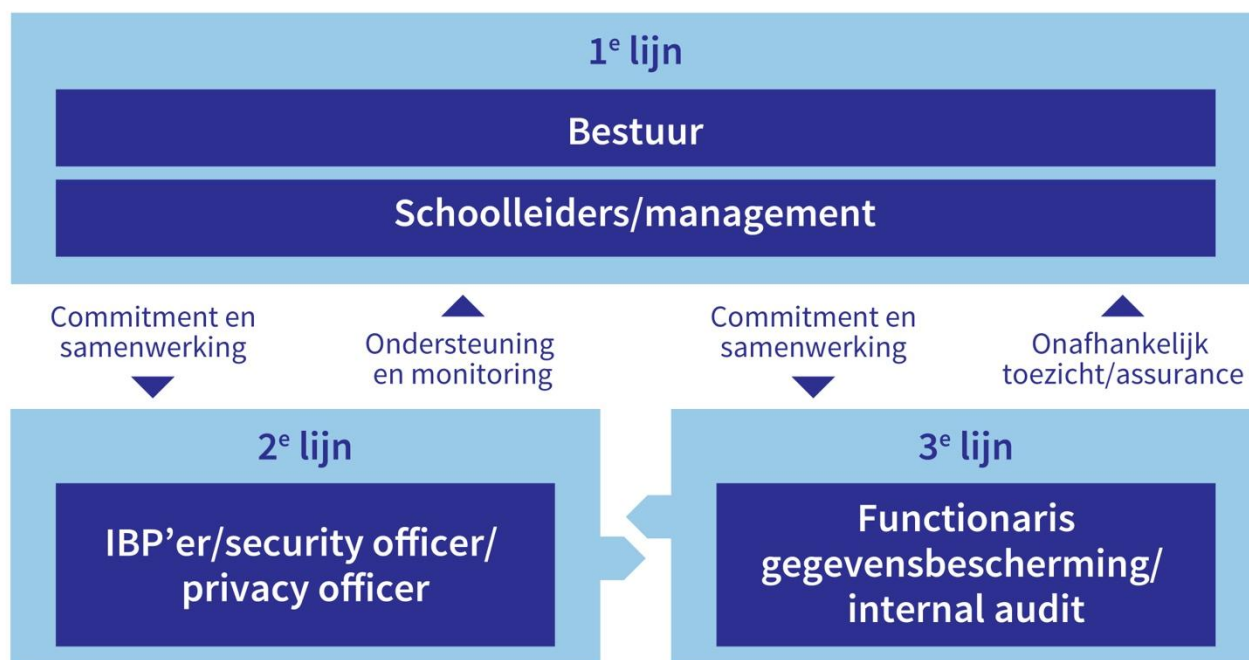
Documentnaam	Beleidsplan IBP	2025-11-04
Auteur	Ricardo Teeuwsen IBP'er	Pagina 8 van 23
Status	Definitief	

principes en standaarden op het gebied van informatiebeveiliging en privacy waaraan Paraat scholen moet voldoen in 2027 voor een digitale veilige schoolomgeving.

Eigenaarschap en verantwoordelijkheden

Dit hoofdstuk beschrijft hoe de verschillende rollen en verantwoordelijkheden met betrekking tot informatiebeveiliging en privacy samenhangen.

Three Lines model



Informatiebeveiliging en privacy bij Paraat scholen is ingericht volgens het Three Lines model (3L-model). Het 3L-model is een leidraad bij het inrichten van de governance van een organisatie binnen het IBP.

Eerste lijn: eindverantwoordelijkheid bij het bestuur

Rollen: De eerste lijn bestaat uit het bestuur, schoolleiders, en het verdere operationele management van Paraat scholen.

Het 3L-model heeft als uitgangspunt dat de eerste lijn verantwoordelijk is voor processen, informatie en systemen van de organisatie, de risico's die hieruit voortvloeien en het treffen van de juiste maatregelen om de risico's te verkleinen. De eerste lijn bestaat uit het bestuur, schoolleiders, en het verdere lijnmanagement van Paraat scholen.

Tweede lijn: adviseren en ondersteunen

Rollen: De tweede lijn bestaat uit Bovenschools ICT, IBP-adviseurs en juridische adviseurs (extern).

Documentnaam	Beleidsplan IBP	2025-11-04
Auteur	Ricardo Teeuwsen IBP'er	Pagina 9 van 23
Status	Definitief	

Naast de eerste lijn moet er een rol zijn die de eerste lijn ondersteunt, adviseert, coördineert en die bewaakt of het management de verantwoordelijkheden ook daadwerkelijk neemt. Dit is de tweede lijn. De tweede lijn bestaat uit Bovenschools ICT, IBP-adviseurs en juridische adviseurs.

Derde lijn: onafhankelijke controle

Rollen: De derde lijn bestaat uit de functionaris gegevensbescherming (FG)

De derde lijn controleert of de eerste en tweede lijn soepel samenwerken en goed functioneren. De derde lijn is onafhankelijk, opereert los van de andere organisatieonderdelen en suggereert waar nodig verbeteringen. De functionaris gegevensbescherming (FG) en de interne auditor vallen binnen de derde lijn. De FG wordt aangesteld door het bestuur en heeft een wettelijk omschreven en onafhankelijke toezichthoudende taak. De FG werkt via een reglement dat door het bestuur wordt vastgesteld.

Medezeggenschap

Paraat scholen betreft de gemeenschappelijke medezeggenschapsraad (GMR) bij besluiten over regelingen en procedures ten aanzien van de bescherming van persoonsgegevens. Het schoolbestuur is eindverantwoordelijk voor het informeren van de gemeenschappelijke medezeggenschapsraad en voor het opstellen van instemmingsprocedures.

Risicomanagement Paraat scholen

Kennis en Afhankelijkheid Medewerkers

Binnen Paraat Scholen vormt de deskundigheid en inzetbaarheid van medewerkers een essentiële schakel in het waarborgen van informatiebeveiliging en de continuïteit van het onderwijs. De organisatie erkent het risico dat ontstaat wanneer cruciale kennis geconcentreerd is bij een beperkt aantal personen. Om deze afhankelijkheid te beperken, wordt een back-upplan opgesteld waarin vervangbaarheid van sleutelrollen wordt geborgd. Medewerkers worden actief gestimuleerd tot het volgen van trainingen en het behalen van relevante certificeringen. Bij in- en uitstroom van personeel worden heldere procedures gevolgd om kennisoverdracht en autorisatiebeheer adequaat af te handelen. Dit is terug te vinden in het personeelshandboek van Paraat scholen.

Bedrijfscontinuïteit

Het waarborgen van de continuïteit van onderwijs- en ondersteuningsprocessen is voor Paraat Scholen van strategisch belang. De organisatie voert periodiek Business Impact Analyses (BIA) uit om de kritieke processen, systemen en functies te identificeren. Regelmatige monitoring zorgen ervoor dat de paraatheid gewaarborgd blijft en dat het continuïteitsbeleid actueel blijft.

Business Impact Analyse (BIA)

De BIA helpt Paraat Scholen bij het prioriteren van processen en systemen op basis van hun impact op het onderwijs en de bedrijfsvoering. De analyse kijkt naar uitvalscenario's en bepaalt hersteltijden (RTO) en maximaal dataverlies (RPO). De inzichten uit deze analyse vormen de basis voor herstelmaatregelen en worden jaarlijks geëvalueerd of na een ernstig incident herzien.

Documentnaam	Beleidsplan IBP	2025-11-04
Auteur	Ricardo Teeuwssen IBP'er	Pagina 10 van 23
Status	Definitief	

Bedrijfscontinuïteitsplan (BCP)

Een BCP is een Bedrijfscontinuïteitsplan dat specifiek is toegespitst op basisscholen en schoolbesturen. Het doel is om ervoor te zorgen dat het onderwijs en de ondersteuning doorgaan of snel worden hersteld bij verstoringen, incidenten of crises.

Back-up en Herstel

Paraat Scholen ziet het maken en beheren van back-ups als een fundamenteel onderdeel van risicobeheersing. Voor alle systemen en data worden op basis van de BIV-classificatie passende back-upvereisten vastgesteld. Er worden periodieke hersteltesten uitgevoerd om de betrouwbaarheid van de back-ups te waarborgen. Bij uitbesteding gelden gelijke eisen voor back-upvoorzieningen als voor interne systemen. Jaarlijks vindt er een evaluatie plaats om de effectiviteit van het back-up- en herstelproces te toetsen en waar nodig bij eventuele wijzigingen zal dit eerder plaatsvinden.

Fysieke Beveiliging

Het doel van fysieke beveiliging is om ongeautoriseerde fysieke toegang tot informatie(systemen), netwerkkapparatuur, leerlinggegevens en overige vertrouwelijke informatie te voorkomen. Door het nemen van passende fysieke maatregelen wordt de kans op verlies, diefstal of misbruik van gegevens beperkt.

Toegangscontrole

- Kantoorruimten, serverkasten en opslagruimtes voor leerlingdossiers zijn altijd afgesloten.
- Sleutels of toegangspasjes worden alleen verstrekt aan geautoriseerd personeel.
- Bezoekers worden altijd aangemeld en begeleid door een medewerker.

Opslag van leerlinggegevens

- Leerlingdossiers op papier worden opgeslagen in afsluitbare archiefkasten in een afgesloten kantoor.
- Digitale informatie is alleen toegankelijk via apparaten met inlogbeveiliging.

Beveiliging van mobiele apparaten

- Laptops, telefoons en tablets worden buiten gebruikstijd opgeslagen in afsluitbare karren of lockers.
- Apparaten blijven niet onbeheerd achter in klaslokalen na lestijd.

Beveiliging gebouw buiten schooltijd

- De school is voorzien van een alarmsysteem dat automatisch wordt ingeschakeld buiten schooluren.
- Conciërges of externe beveiligingsdiensten voeren regelmatig controlerondes uit.

Documentnaam	Beleidsplan IBP	2025-11-04
Auteur	Ricardo Teeuwssen IBP'er	Pagina 11 van 23
Status	Definitief	

Fysieke bescherming van netwerkkaparaatuur

- Routers, switches en servers zijn opgeborgen in een afgesloten patchkast of serverkast.
- De kast is alleen toegankelijk voor geautoriseerde medewerkers, zoals ICT-beheerders.

Systeem- en Data-eigenaarschap en Configuratiebeheer

Voor effectief beheer van IT-processen is het noodzakelijk om helder inzicht te hebben in de gebruikte systemen en de bijbehorende verantwoordelijkheden. Paraat Scholen kent per systeem een eigenaar toe, die verantwoordelijk is voor het beheer, het onderhoud en de naleving van beleidsregels. Deze informatie wordt vastgelegd in een Configuratie Management Database (CMDB). Daarnaast worden processen beschreven in het verwerkingsregister, waar ook het proceseigenaarschap wordt belegd. Data-eigenaarschap wordt gekoppeld aan het systeem waarin de data zich bevinden.

Classificatie van Systemen en Data

Binnen Paraat Scholen wordt voor ieder informatiesysteem beoordeeld welke beveiligingseisen noodzakelijk zijn aan de hand van het BIV-classificatiemodel. Hierbij worden de mate van Beschikbaarheid, Integriteit en Vertrouwelijkheid per systeem vastgesteld. De classificatie is systeemgericht en vindt plaats vóór de ingebruikname van het systeem. De uitkomst bepaalt welke beveiligingsmaatregelen vereist zijn en wordt geregistreerd in de CMDB.

Documentnaam	Beleidsplan IBP	2025-11-04
Auteur	Ricardo Teeuwsen IBP'er	Pagina 12 van 23
Status	Definitief	

BIV-classificatie

Systeem	Beschikbaarheid	Integriteit	Vertrouwelijkheid	Toelichting
Leerlingadministratiesysteem (LAS) (ParnasSys)	Hoog	Hoog	Hoog	Essentieel voor onderwijscontinuïteit; bevat persoonsgegevens en onderwijsresultaten.
Financieel systeem	Gemiddeld	Hoog	Hoog	Verwerking van betalingen en salarissen; gegevens moeten correct en beschermd zijn.
E-mailomgeving (Microsoft 365/Google)	Gemiddeld	Gemiddeld	Gemiddeld	Belangrijk voor communicatie; geen structurele opslag van gevoelige gegevens.
Schoolwebsite	Laag	Laag	Laag	Openbare informatievoorziening; geen verwerking van persoonsgegevens.
HR-systeem	Gemiddeld	Hoog	Hoog	Bevat personeelsdossiers, contractinformatie en medische gegevens.
Digitale leeromgeving (bijv. Basispoort)	Hoog	Gemiddeld	Gemiddeld	Dagelijks onderwijs afhankelijk; beperkte opslag van vertrouwelijke gegevens.
Netwerk en wifi-infrastructuur	Hoog	Gemiddeld	Laag	Cruciaal voor continuïteit onderwijs en verbinding met cloudsysteem.
Cloudopslag (Microsoft 365)	Hoog	Hoog	Hoog	Opslag van beleidsstukken, leerlingdossiers en contracten.

Deze classificatie helpt bij het bepalen van de noodzakelijke beveiligingsmaatregelen per systeemtype. De afweging per systeem gebeurt gestructureerd en wordt afgestemd op het risico.

Documentnaam	Beleidsplan IBP	2025-11-04
Auteur	Ricardo Teeuwsen IBP'er	Pagina 13 van 23
Status	Definitief	

Securitybaseline

Binnen Paraat Scholen is een securitybaseline opgesteld voor alle IT-systemen die de minimale beveiligingsmaatregelen definieert. Deze baseline zorgt ervoor dat systemen voldoen aan de basisvereisten voor informatiebeveiliging, waaronder wachtwoordbeleid, toegangscontrole, netwerksegmentatie, versleuteling en logging. De naleving van deze baseline wordt periodiek getoetst, en afwijkingen moeten gemotiveerd en vastgelegd worden. Het beleid wordt jaarlijks geëvalueerd en indien nodig aangepast op basis van technologische en organisatorische ontwikkelingen.

Bewustwording

Het vergroten van het bewustzijn onder medewerkers over informatiebeveiliging is een structureel aandachtspunt. Paraat Scholen hanteert een bewustwordingsprogramma waarin training, voorlichting en communicatie over risico's en gewenst gedrag zijn opgenomen. Medewerkers worden regelmatig geïnformeerd over actuele dreigingen, phishingcampagnes en hun rol in het beschermen van gegevens. Dit programma wordt jaarlijks geëvalueerd en geactualiseerd. De resultaten worden gebruikt om gerichte interventies te ontwikkelen. Deelname aan bewustwordingsactiviteiten wordt gevolgd en besproken in bijvoorbeeld teamvergaderingen.

Incident- en Probleemmanagement

Incidenten en terugkerende problemen binnen de informatievoorziening worden centraal gemeld en vastgelegd in een incidentenregister. Elk incident wordt geclassificeerd, geanalyseerd en opgevolgd. Indien nodig wordt opgeschaald naar een crisisteam. Het proces is gericht op snelle detectie, herstel en structurele verbetering. Probleemmanagement richt zich op de analyse van terugkerende incidenten om root causes weg te nemen.

Voor elk informatiebeveiligingsincident wordt een standaardprocedure gevolgd waarin de volgende stappen zijn opgenomen:

1. Eerste melding en classificatie (via avg@paraatscholen.nl).
2. Eerste beoordeling door Functionaris Gegevensbescherming.
3. Escalatie indien nodig.
4. Analyse van oorzaak en getroffen maatregelen.
5. Evaluatie en documentatie van lessons learned.

Een incidentrapport wordt verplicht opgesteld bij datalekken en herhaalde incidenten en opgenomen in het incidentregister.

Risicomanagement Leveranciers

Paraat Scholen stelt eisen aan leveranciers op het gebied van informatiebeveiliging, passend bij de BIV-classificatie van het uitbestede systeem. Bij de selectie van leveranciers wordt vooraf bepaald aan welke beveiligingsmaatregelen voldaan moet worden. Afspraken hierover worden vastgelegd in verwerkersovereenkomsten en contracten. Periodiek worden leveranciers getoetst op naleving van deze eisen.

Documentnaam	Beleidsplan IBP	2025-11-04
Auteur	Ricardo Teeuwsen IBP'er	Pagina 14 van 23
Status	Definitief	

Paraat Scholen voert periodiek leveranciersbeoordelingen uit op basis van vooraf opgestelde criteria, waaronder:

- Naleving van verwerkersovereenkomsten;
- beveiligingsmaatregelen;
- resultaten van audits;
- incidenthistorie.

Bij beëindiging van contracten wordt geborgd dat alle data correct wordt verwijderd of overgedragen conform afspraken. Er is een standaard exit-procedure die jaarlijks wordt herzien.

Werkplekken en Mobiele Apparaten

Informatie wordt ontsloten via uiteenlopende apparaten zoals laptops, tablets en smartphones. Paraat Scholen hanteert beleid en richtlijnen voor het veilige gebruik hiervan, waaronder schermvergrendeling, encryptie, automatische updates en beheer op afstand. Medewerkers worden geïnformeerd over verantwoord gebruik. Medewerkers maken gebruik van de door Paraat beschikbaar gestelde apparaten voor de uitvoering van hun werkzaamheden. Het gebruik van privéapparaten voor werkdoeleinden wordt beperkt tot het minimale, om de informatiebeveiliging te waarborgen en controle over de werkomgeving te behouden.

Identiteits- en Toegangsbeheer

Toegangsbeheer wordt ingericht volgens het need-to-know-principe. Rollen en rechten worden afgestemd op functies en taken. Bij indiensttreding, functiewijziging en uitdiensttreding worden autorisaties automatisch aangepast. Toegang tot gevoelige systemen wordt waar mogelijk

Vulnerabilitymanagement en Pentesting

Kwetsbaarheden binnen systemen worden actief gemonitord en verholpen. Paraat Scholen maakt gebruik van automatische kwetsbaarheidsscans, in combinatie met periodieke handmatige tests. Voor kritieke systemen wordt om de twee/drie jaar een penetratietest uitgevoerd. Bevindingen worden geregistreerd en opgevolgd.

Patchmanagement

Updates en beveiligingspatches worden binnen vastgestelde termijnen getest en geïmplementeerd. De urgentie van updates wordt mede bepaald door de BIV-classificatie van het systeem. Automatische updateprocessen zorgen ervoor dat veelgebruikte software altijd up-to-date is. Het patchbeleid is onderdeel van het algemene beheerproces.

Logging

Activiteiten binnen systemen worden gelogd voor het opsporen van incidenten en het uitvoeren van audits. Logbestanden worden centraal opgeslagen, beveiligd en periodiek geanalyseerd. De mate van logging is afhankelijk van de gevoeligheid van het systeem en de aard van de verwerkte gegevens.

Digitaal Sleutelbeheer

Voor het beschermen van vertrouwelijke gegevens maakt Paraat Scholen gebruik van encryptie. Digitale sleutels die voor encryptie worden gebruikt, worden zorgvuldig beheerd in een daartoe

Documentnaam	Beleidsplan IBP	2025-11-04
Auteur	Ricardo Teeuwsen IBP'er	Pagina 15 van 23
Status	Definitief	

ingericht sleutelbeheerproces. Dit proces beschrijft hoe sleutels worden aangemaakt, opgeslagen, vervangen en verwijderd. Daarnaast worden digitale certificaten ingezet voor verificatie en integriteitscontrole.

Uitgangspunten privacy

Het algemene uitgangspunt in dit IBP-beleid is dat persoonsgegevens in overeenstemming met de AVG en gerelateerde wet- en regelgeving op zorgvuldige wijze worden verwerkt. Om aan dit uitgangspunt te voldoen verwerkt Paraat scholen persoonsgegevens in overeenstemming met de privacyvuistregels die in verderop in dit hoofdstuk worden uiteengezet. Paraat scholen treft verdiepende maatregelen om de beleidsthema's in dit IBP-beleid in te vullen.

Persoonsgegevens

Persoonsgegevens zijn gegevens die direct of indirect over iemand gaan en dus naar een persoon te herleiden zijn, zoals een naam of e-mailadres. Naast gewone persoonsgegevens - denk aan contactgegevens en onderwijsnummers - onderscheidt de AVG bijzondere persoonsgegevens en strafrechtelijke persoonsgegevens. Daarnaast bestaat een categorie 'gevoelige' persoonsgegevens die niet expliciet in de AVG is benoemd. Dit zijn persoonsgegevens die vanwege hun aard privacygevoelig zijn en daarom extra bescherming verdienen.

- **Bijzondere persoonsgegevens** zijn gegevens die te maken hebben met bijvoorbeeld ras of etnische afkomst, gezondheid, religie of seksueel gedrag. De verwerking van deze gegevens is verboden, tenzij een wettelijke uitzondering bestaat zoals toestemming van de betrokkene.
- **Strafrechtelijke gegevens** zijn gegevens die te maken hebben met strafrechtelijke veroordelingen en strafbare feiten. De verwerking van deze gegevens is ook verboden, tenzij hiervoor een wettelijke uitzondering geldt.
- **Gevoelige persoonsgegevens** zijn gegevens die een groter privacyrisico vormen dan gewone persoonsgegevens. Denk aan financiële gegevens, burgerservicenummers (BSN), beoordelingen of gegevens van kwetsbare leerlingen.

NB: Nummers ter identificatie van een persoon, zoals het BSN, mogen alleen worden gebruikt voor specifieke doeleinden die in de wet zijn vastgelegd. Een onderwijsnummer (persoonsgebonden nummer) is gelijk aan het BSN.

Privacyvuistregels

Bij het verwerken van persoonsgegevens houdt Paraat scholen rekening met onderstaande vuistregels. Door deze basisprincipes te volgen zorgen we ervoor dat we kunnen voldoen aan de AVG.

We verwerken persoonsgegevens rechtmatig en transparant

Paraat scholen verzamelt en gebruikt persoonsgegevens op een eerlijke en transparante manier. Persoonsgegevens worden alleen verwerkt als daarvoor een wettelijke grondslag bestaat in de AVG. We leggen altijd duidelijk uit waarom we bepaalde gegevens nodig hebben, wat we ermee doen en hoe lang we deze gegevens bewaren. Daarom informeren we ouders en leerlingen tijdig

Documentnaam	Beleidsplan IBP	2025-11-04
Auteur	Ricardo Teeuwsen IBP'er	Pagina 16 van 23
Status	Definitief	

over het gebruik van hun persoonsgegevens, via een transparante privacyverklaring. Dit gebeurt bijvoorbeeld op het moment van inschrijving van een leerling.

We verwerken persoonsgegevens voor specifieke doeleinden

Paraat scholen verwerkt persoonsgegevens alleen wanneer vooraf de specifieke doeleinden voor de verwerking zijn bepaald. Deze doeleinden worden vastgelegd. Persoonsgegevens worden niet voor andere, niet-verenigbare, doelen verwerkt. We zullen dus niet persoonsgegevens verzamelen omdat die wellicht ooit van pas gaan komen. We doen dit alleen met vooraf bepaalde, duidelijke en gerechtvaardigde doelen, zoals het plannen van onderwijs en communiceren met leerlingen en ouders over de voortgang en schoolactiviteiten.

We verwerken alleen noodzakelijke persoonsgegevens

Paraat scholen verzamelt alleen persoonsgegevens die noodzakelijk zijn voor het doel waarvoor ze worden verwerkt. We vragen dus niet om meer gegevens dan we daadwerkelijk nodig hebben en hanteren hierbij het uitgangspunt 'zo min mogelijk'. We onderzoeken altijd of we met minder gegevens of enkel met anonieme gegevens kunnen werken. Zo vragen we bij de inschrijving van een leerling alleen om de gegevens die relevant zijn voor het kunnen bieden van onderwijs en bewaren we geen overbodige gegevens die niet nodig zijn voor onze schoolactiviteiten.

We zorgen dat persoonsgegevens juist en actueel zijn

Paraat scholen treft maatregelen om ervoor te zorgen dat persoonsgegevens correct en actueel zijn. Onjuiste of achterhaalde gegevens worden geactualiseerd of verwijderd. Leerlingen en ouders kunnen op een laagdrempelige manier doorgeven dat persoonsgegevens incorrect zijn en/of gewijzigd moeten worden. Onze processen en systemen worden zo ingericht dat de juistheid van gegevens zoveel mogelijk wordt afgedwongen en gecontroleerd.

We bewaren persoonsgegevens niet langer dan nodig

Paraat scholen bewaart persoonsgegevens niet langer dan noodzakelijk is voor het doel waarvoor ze zijn verzameld. Zodra gegevens niet meer nodig zijn, worden ze verwijderd of geanonimiseerd. We houden ons hierbij aan vooraf vastgestelde bewaartermijnen. Zo wordt het leerlingendossier (inclusief rapporten en schoolprestaties) na uitschrijving van een leerling niet langer bewaard dan nodig is voor administratieve en onderwijsdoeleinden en dus zo spoedig mogelijk verwijderd, in ieder geval binnen 2 jaar na uitschrijving.

We zorgen voor een passende bescherming van persoonsgegevens

We kunnen de privacy van leerlingen, ouders en medewerkers alleen goed beschermen als we op een veilige manier met hun persoonsgegevens omgaan. We zijn daarom verantwoordelijk voor het treffen van passende technische en organisatorische beveiligingsmaatregelen. Die maatregelen moeten ervoor zorgen dat de persoonsgegevens op een passende wijze worden beveiligd en worden beschermd tegen verlies, vernietiging, beschadiging of onrechtmatige verwerking. Dit doen we bijvoorbeeld door het gebruik van veilige systemen voor de opslag van leerlinggegevens en het opleiden van personeel in het veilig omgaan met gevoelige gegevens.

We kunnen aantonen dat we voldoen aan de AVG

We zijn verantwoordelijk voor het naleven van bovengenoemde vuistregels en kunnen daarmee aantonen dat we voldoen aan de belangrijkste uitgangspunten van de AVG. Dit doen we bijvoorbeeld door het bijhouden van een verwerkingsregister en het uitvoeren van *Data Protection Impact Assessments* (DPIA's) voor gegevensverwerkingen met een hoog privacyrisico.

Documentnaam	Beleidsplan IBP	2025-11-04
Auteur	Ricardo Teeuwse IBP'er	Pagina 17 van 23
Status	Definitief	

We kunnen ons ethisch verantwoorden

Bij het beoordelen van verwerkingen van persoonsgegevens houdt Paraat scholen niet alleen rekening met de vereisten uit de AVG (*'mogen we dit?'*), maar nadrukkelijk ook met ethische aspecten (*'willen we dit?'*). Het gaat hierbij dus niet om de vraag of we iets 'mogen' of 'kunnen', maar juist om de vraag of we iets zouden moeten 'willen' als school. Ethische aspecten spelen in het bijzonder een rol bij verwerkingen die privacyrisico's kunnen opleveren, bijvoorbeeld bij het gebruik van meekijksoftware of schermcontroles. Dit moet ook worden gezien vanuit een ethisch afwegingskader. We stellen ons dan ook eerst de vraag of we het kunnen uitleggen aan leerlingen en ouders.

Beleidsthema's privacy

Verwerkingsregister

Paraat scholen heeft maatregelen getroffen om aantoonbaar te voldoen aan de eisen uit de AVG. Dit houdt onder meer in dat Paraat scholen kan aantonen dat de verwerking van persoonsgegevens voldoet aan de uitgangspunten uit de AVG. Paraat scholen geeft onder meer invulling aan haar verantwoordingsplicht door een overzicht bij te houden met informatie over de persoonsgegevens die zij verwerkt. Dit heet het verwerkingsregister. Dit register bevat bijvoorbeeld informatie over de leerlingenadministratie of het HR-systeem. Het bijhouden van het verwerkingsregister zorgt voor een goed overzicht van welke persoonsgegevens worden verwerkt en met welk doel dit gebeurt. Het register stelt Paraat scholen in staat te voldoen aan haar verantwoordingsplicht. Het verwerkingsregister bevat van afzonderlijke verwerkingsactiviteiten informatie over onder meer de doeleinden voor de verwerking, de toepasselijke grondslag onder de AVG, een beschrijving van de betrokkenen, een beschrijving van de persoonsgegevens, de toepasselijke bewaartermijnen en de ontvangers waarmee persoonsgegevens worden gedeeld.

Legitiem doel en doelbinding

Persoonsgegevens worden alleen verwerkt als een specifiek, vooraf bepaald doel is vastgesteld door Paraat scholen. Dit doel moet duidelijk en in begrijpelijke taal aan de betrokkenen worden uitgelegd. Persoonsgegevens mogen niet voor andere doeleinden worden gebruikt.

Paraat scholen verwerkt persoonsgegevens om haar verplichtingen als onderwijsinstelling na te kunnen komen. Het schoolbestuur verwerkt persoonsgegevens in de eerste plaats om onderwijs te kunnen bieden aan haar leerlingen en om activiteiten die hieraan ondersteunend zijn te kunnen uitvoeren. Hierbij valt te denken aan verwerkingen in het kader van het aanmeldproces, om te communiceren met leerlingen en ouders/verzorgers, het bijhouden van de leerlingenadministratie, het maken van roosters en om de voortgang bij te houden. Ook verwerkt het schoolbestuur persoonsgegevens van haar medewerkers in haar rol als werkgever. Paraat scholen verwerkt bij deze werkzaamheden verschillende (categorieën) persoonsgegevens, waaronder contactgegevens, naam, geboortedatum en gegevens betreffende de aard en het verloop van het onderwijs. Paraat scholen verwerkt deze persoonsgegevens op basis van grondslagen uit de AVG, bijvoorbeeld omdat sprake is van een wettelijke taak of verplichting, een gerechtvaardigd belang of op basis van toestemming.

Documentnaam	Beleidsplan IBP	2025-11-04
Auteur	Ricardo Teeuwsen IBP'er	Pagina 18 van 23
Status	Definitief	

Als gegevens toch voor een ander doel nodig zijn, dan mag dit alleen als dat doel verenigbaar is met het oorspronkelijke doel. Om te bepalen of dit het geval is, moet onder andere worden gekeken naar:

- De relatie tussen het nieuwe en het oorspronkelijke doel.
- De context waarin de gegevens zijn verzameld en de redelijke verwachtingen van de betrokkenen.
- Het soort persoonsgegevens; gevoelige gegevens verdienen extra bescherming.
- De mogelijke gevolgen voor betrokkenen.
- Bescherming van de gegevens, zoals versleuteling of pseudonimiseren.

Voor elke nieuwe verwerking moet Paraat scholen de rechtmatigheid, zorgvuldigheid en noodzaak opnieuw beoordelen. De specifieke doeleinden worden voorafgaand aan de verwerking bepaald en vermeld in de privacyverklaring om betrokken te informeren. Ook worden de doeleinden opgenomen in het verwerkingsregister. Voordat gegevens voor een ander doel worden gebruikt, vindt overleg plaats met de IBP adviseur en indien nodig ook met de functionaris gegevensbescherming.

Grondslag

Paraat scholen moet voor iedere verwerking van persoonsgegevens een geldige reden hebben. De AVG noemt dit een grondslag. Paraat scholen verwerkt persoonsgegevens alleen op basis van de in de AVG genoemde grondslagen:

- De betrokkene heeft **toestemming** verleend, bijvoorbeeld voor het maken en delen van foto's of video's.
- De verwerking is noodzakelijk voor de **uitvoering van een overeenkomst** waarbij de betrokkene partij is, bijvoorbeeld het verwerken van salaris om de arbeidsovereenkomst met werknemers na te komen.
- De verwerking is noodzakelijk om te voldoen aan een **wettelijke verplichting**, bijvoorbeeld het delen van salarisinformatie met de Belastingdienst voor de uitvoering van de belastingwetgeving.
- De verwerking is noodzakelijk om **de vitale belangen** van de betrokkene te beschermen, bijvoorbeeld bij een levensbedreigende situatie waarbij het noodzakelijk is dat bepaalde gegevens van een leerling acuut aan hulpverleners moeten worden doorgegeven.
- De verwerking is noodzakelijk om uitvoering te geven aan een **taak van algemeen belang**, hierbij gaat het om wettelijk vastgestelde taken en bevoegdheden. Zo heeft Paraat scholen de wettelijke taak om onderwijs te bieden.
- De verwerking is noodzakelijk voor de behartiging van een **gerechtvaardigd belang** van Paraat scholen of van een derde. Denk hierbij aan het verwerken van medewerkersgegevens voor het opstellen van managementrapportages ten behoeve van beleidsontwikkeling of het gebruik van bewakingscamera's op het schoolplein.

Documentnaam	Beleidsplan IBP	2025-11-04
Auteur	Ricardo Teeuwsen IBP'er	Pagina 19 van 23
Status	Definitief	

De toepasselijke grondslag wordt vooraf vastgesteld, bijvoorbeeld middels een DPIA, en benoemd in de privacyverklaring om betrokken te informeren. Ook wordt de toepasselijke grondslag opgenomen in het verwerkingsregister.

Informatieplicht

Paraat scholen verwerkt persoonsgegevens op een behoorlijke en transparante manier. Dit is in begrijpelijke taal inzichtelijk voor de betrokkenen. Paraat scholen informeert leerlingen en medewerkers voorafgaand aan de gegevensverwerking op transparante wijze via een duidelijke privacyverklaring. Deze privacyverklaring wordt gepubliceerd op de website. Daarnaast informeert de school medewerkers en sollicitanten ook via een aparte privacyverklaring. Hiermee zorgt Paraat scholen ervoor dat betrokkenen weten welke persoonsgegevens worden verwerkt en voor welke doeleinden dit gebeurt. Ook zijn ze op de hoogte van de rechten die ze hebben.

Wordt gebruikt gemaakt van geautomatiseerde besluitvorming of profilering? Dan gelden extra strenge regels, ook op het gebied van transparantie. Dat betekent onder andere dat medewerkers en leerlingen goed moeten worden geïnformeerd over het gebruik hiervan en duidelijk moet worden uitgelegd op basis van welke criteria het besluit tot stand is gekomen. Ook moet de mogelijkheid bestaan een nieuw besluit te nemen waarbij een mens de gegevens beoordeelt. Op die manier beschermen we medewerkers en leerlingen tegen onrechtmatige verwerking.

Toestemming

Bij het gebruik van toestemming als grondslag gelden een aantal voorwaarden:

- Toestemming moet op een begrijpelijke en toegankelijke manier worden gevraagd, in duidelijke taal en niet verborgen in algemene voorwaarden of lange teksten.
- Toestemming moet vrijwillig worden gegeven en moet ook weer gemakkelijk ingetrokken kunnen worden.
- Paraat scholen moet kunnen aantonen dat toestemming is verkregen, bijvoorbeeld door logs of ondertekende formulieren.
- Voor kinderen onder de 16 jaar moet een wettelijke vertegenwoordiger toestemming geven. Dit geldt ook voor personen onder curatele, bewind of mentorschap. Paraat scholen verifieert of deze vertegenwoordiger daadwerkelijk toestemming heeft gegeven.

Leerlingen (of hun wettelijke vertegenwoordigers) worden in bepaalde situaties om toestemming gevraagd. Denk aan de situatie dat Paraat scholen foto's of video's van leerlingen maakt en publiceert. Dit mag alleen als de school vooraf toestemming heeft verkregen. Omdat een gezagsrelatie bestaat tussen Paraat scholen en haar leerlingen en medewerkers, moet goed worden beargumenteerd waarom toestemming in specifieke gevallen in vrijheid kan worden gegeven. Paraat scholen gaat daarom terughoudend om met het gebruik van deze grondslag. Voordat toestemming als grondslag wordt gebruikt, vindt overleg plaats met de privacy officer en indien nodig ook met de functionaris gegevensbescherming.

Documentnaam	Beleidsplan IBP	2025-11-04
Auteur	Ricardo Teeuwsen IBP'er	Pagina 20 van 23
Status	Definitief	

Privacy by design en privacy by default

Privacy by design betekent dat Paraat scholen bij de ontwikkeling, het ontwerp, de selectie en het gebruik van toepassingen, diensten en producten zo vroeg mogelijk rekening houdt met privacyrisico's en passende waarborgen inbouwt om de privacy van betrokkenen te beschermen. Neemt Paraat scholen bijvoorbeeld een leerlingvolgsysteem in gebruik? Dan moet in een vroeg stadium al worden nagedacht over passende toegangsbeperkingen. Leerkrachten en onderwijsassistenten hebben alleen inzicht in de noodzakelijke gegevens van hun eigen leerlingen. *Privacy by default* betekent dat de standaardinstellingen van een product, dienst of proces op de meest privacyvriendelijke instelling staan. Maakt Paraat scholen bijvoorbeeld een profiel aan op sociale media? Dan mag dit profiel niet standaard openbaar zichtbaar zijn.

Hiermee zorgt Paraat scholen ervoor dat zo vroeg mogelijk rekening wordt gehouden met privacybeginselen en op die manier privacyrisico's tijdig worden gemitigeerd.

Dataminimalisatie

Paraat scholen verzamelt alleen gegevens die noodzakelijk zijn voor het doel dat voorafgaand aan de verwerking is vastgesteld. De verzamelde gegevens dienen toereikend, ter zake dienend en niet bovenmatig te zijn. Hiermee voorkomt Paraat scholen dat te veel gegevens worden verwerkt. Bij de aanmelding van een leerling verzamelt Paraat scholen bijvoorbeeld alleen de informatie die nodig is om de leerling op de juiste manier in te schrijven. Denk aan naam, geboortedatum, adres en contactgegevens van ouders/verzorgers. Extra informatie, zoals het beroep van de ouders, is niet relevant voor de inschrijving en hoort daarom niet te worden verzameld. Daarnaast moet de verwerking van persoonsgegevens op de minst ingrijpende wijze plaatsvinden. Als het beoogde doel op een privacyvriendelijkere manier kan worden bereikt, dan kiest Paraat scholen hiervoor. Op deze manier voldoet Paraat scholen eveneens aan de principes van *privacy by design*.

Bewaartermijnen

Persoonsgegevens worden niet langer bewaard dan noodzakelijk voor de doeleinden waarvoor zij zijn verzameld. Dit gebeurt in overeenstemming met het bewaar- en vernietigingsbeleid van Paraat scholen. Na het verlopen van de toepasselijke bewaartermijnen zorgt Paraat scholen ervoor dat persoonsgegevens tijdig worden vernietigd (of geanonimiseerd). Hierdoor worden persoonsgegevens beter beschermd tegen onnodige verwerking en datalekken. Zo worden bijvoorbeeld overzichten van schoolprestaties en rapporten uiterlijk tot 2 jaar na uitschrijving van een leerling bewaard. Het schooladvies wordt tot uiterlijk 5 jaar na uitschrijving van een leerling bewaard.

Afhandelen van datalekken

Voorbeelden van datalekken zijn een gestolen laptop, telefoon, een verloren usb-stick, een e-mail of een bericht via Parro/Klasbord met persoonsgegevens. Datalekken moeten direct worden gemeld via avg@paraatscholen.nl en bij de FG en geregistreerd in het interne register voor beveiligingsincidenten en datalekken. Risicovolle datalekken moeten worden gemeld aan de Autoriteit Persoonsgegevens en ook aan de betrokkenen als het datalek waarschijnlijk een hoog risico voor hen oplevert. De FG beoordeelt of zo'n melding nodig is. Dit gebeurt als het nodig is in samenspraak met de bestuurder.

Documentnaam	Beleidsplan IBP	2025-11-04
Auteur	Ricardo Teeuwsen IBP'er	Pagina 21 van 23
Status	Definitief	

Data Protection Impact Assessment

Voor elke nieuwe verwerking van persoonsgegevens, bijvoorbeeld een nieuw proces, technologie of applicatie, controleert Paraat scholen of de privacybeginselen uit de AVG worden nageleefd. Bij verwerkingen met een hoog privacyrisico wordt eerst een *Data Protection Impact Assessment* (DPIA) uitgevoerd. Een DPIA brengt in kaart hoe groot de kans is dat de privacy van betrokkenen wordt geschaad, waar de risico's liggen en welke gevolgen dit kan hebben. Op basis van de uitkomsten van de DPIA neemt Paraat scholen maatregelen om deze risico's te mitigeren.

Uitwisseling persoonsgegevens

Een verwerker is een partij die in opdracht van Paraat scholen persoonsgegevens verwerkt, zoals een leverancier van een leerlingadministratiesysteem. Als Paraat scholen een verwerker inschakelt om persoonsgegevens te verwerken, dan worden privacyafspraken vastgelegd in een verwerkersovereenkomst. Bepaalt Paraat scholen samen met één of meerdere partijen het doel en middelen voor de verwerking van persoonsgegevens? Dan is sprake van een zogenaamde gezamenlijke verwerkingsverantwoordelijkheid. In dat geval worden ook contractuele afspraken gemaakt rondom de zorgvuldige en veilige verwerking van gegevens.

Persoonsgegevens kunnen ook beschikbaar worden gesteld aan partijen die niet als verwerkers worden aangemerkt, maar als 'derden'. Deze derden verwerken persoonsgegevens niet in opdracht van een verwerkingsverantwoordelijke, maar voor hun eigen doel. Een verwerkersovereenkomst is daarom ook niet nodig, maar er moet wel een grondslag bestaan om de persoonsgegevens te delen. Denk aan de situatie waarin Paraat scholen gegevens over medewerkers deelt met de Belastingdienst ten behoeve van de loonaangifte. De Belastingdienst verwerkt deze gegevens voor haar eigen wettelijke doeleinden en handelt niet als verwerker.

Gegevensverwerking buiten de EER

Schakelt Paraat scholen een verwerker in uit een land buiten de Europese Economische Ruimte (EER) dat geen passend beschermingsniveau biedt? Dan gelden aanvullende voorwaarden. Bij een gegevensdeling buiten de EER moeten namelijk (juridische, technische en organisatorische) waarborgen zijn genomen om het beschermingsniveau ook buiten de EER te laten voldoen aan de AVG, zodat de persoonsgegevens voldoende beschermd blijven. Om dit te bereiken is meer nodig dan alleen het sluiten van een verwerkersovereenkomst. In dat geval maakt Paraat scholen gebruik van de Europese modelcontracten, de zogenaamde 'Standard Contractual Clauses', en neemt Paraat scholen aanvullende risicogebaseerde beveiligingsmaatregelen. Ook vindt voorafgaand aan de gegevensdeling afstemming plaats met de privacy officer en afdeling informatiebeveiliging om te beoordelen of de getroffen maatregelen voldoende zijn.

NB: De bepalingen van de meest recente versie van het convenant 'Digitale onderwijsmiddelen en privacy' zijn leidend bij het maken van afspraken met leveranciers, die als verwerkers in opdracht van de school persoonsgegevens verwerken.

Rechten van betrokkenen

Betrokkenen hebben op grond van de AVG recht op controle op de verwerking van hun persoonsgegevens. Een betrokkene kan onder andere gebruikmaken van het recht op inzage, rectificatie, verwijdering en bezwaar. Leerlingen, leraren en andere medewerkers kunnen een verzoek tot uitoefening van deze rechten indienen via: avg@paraatscholen.nl Ook hebben betrokkenen het recht een klacht in te dienen bij de Autoriteit Persoonsgegevens.

Documentnaam	Beleidsplan IBP	2025-11-04
Auteur	Ricardo Teeuwsen IBP'er	Pagina 22 van 23
Status	Definitief	

Paraat scholen draagt er zorg voor dat de informatie over het uitoefenen van deze rechten op een transparante manier is verstrekt aan betrokkenen via een privacyverklaring. Paraat scholen zal binnen de wettelijke termijnen, uiterlijk binnen één maand, schriftelijk reageren op het verzoek. In uitzonderlijke situaties kan de reactietermijn worden verlengd, maar dan wordt dit wel binnen een maand gecommuniceerd. Voor AVG-verzoeken geldt een identificatieplicht, zodat de identiteit van de verzoeker kan worden vastgesteld. Hiertoe kan Paraat scholen om extra informatie verzoeken, maar zal hierbij terughoudend zijn met het verzoeken om een kopie identiteitsbewijs.

Verantwoording IBP

Naleving AVG

Er vindt toezicht plaats door Paraat scholen op de naleving van de normen uit dit beleid. Van belang is dat Functionaris gegevensbescherming zijn verantwoordelijkheid nemen en medewerkers aanspreken in geval van tekortkomingen. Paraat scholen besteedt in dit verband actief aandacht aan informatiebeveiliging en privacy bij de aanstelling van medewerkers, tijdens functioneringsgesprek via bewustwordingscampagnes.

Mocht de naleving van dit beleid ernstig tekortschieten, dan kan Paraat scholen de betrokken verantwoordelijke medewerkers maatregelen opleggen binnen de kaders van de CAO en toepasselijke wetgeving. Voor toezicht op de naleving van de AVG vervult de functionaris gegevensbescherming (FG) een belangrijke rol. De FG kan bijvoorbeeld informatie verzamelen over gegevensverwerkingen en beoordelen of deze aan de AVG voldoen. Ook kan de FG adviezen en aanbevelingen verschaffen aan Paraat scholen.

Rapportage

Paraat scholen heeft de verantwoordelijkheid om het IBP-beleid formeel goed te keuren en te monitoren of het IBP-beleid door de organisatie wordt toegepast. Periodiek jaarlijks of bij wetswijziging wordt hierover eerder gerapporteerd in BDS.

Beleidsherziening

Het IBP-beleid wordt door Paraat scholen eenmaal per jaar getoetst en indien nodig herzien. Bij een substantiële wijziging van het IBP-beleid of in geval van belangrijke ontwikkelingen of veranderingen in wet- en regelgeving, volgt er indien nodig een beleidswijziging.

Documentnaam	Beleidsplan IBP	2025-11-04
Auteur	Ricardo Teeuwsen IBP'er	Pagina 23 van 23
Status	Definitief	