SWV Helmond-Peelland PO

Beleid Informatiebeveiliging en Privacy

Laatst bijgewerkt: 25 november 2024

vastgesteld op: 21 januari 2025

Inhoud

INLEIDING

Het SWV Helmond Peelland PO voert taken uit in het kader van de wetgeving Passend Onderwijs, die zijn beschreven en vastgelegd in het ondersteuningsplan. Het SWV kan deze taken alleen uitvoeren op basis van persoonsgegevens van kinderen die het betreft. Deze gegevens worden door ons verwerkt met software, apparatuur en andere middelen.
Ook is SWV werk- en opdrachtgever en beschikt het vanuit deze hoedanigheid over persoonsgegevens van haar medewerkers.

Vanwege het werken met persoonsgegevens is het SWV gehouden aan de Algemene Verordening Gegevensbescherming (AVG). Daartoe wil het SWV beleid formuleren voor InformatieBeveiliging en Privacy (IBP). In dit document beschrijven wij ons IBP-beleid. We gaan in op de uitgangspunten en indicatoren en werken uit welke maatregelen we nemen om aan de eisen van de AVG te voldoen.

Hoofdstuk 1 Waarom informatiebeveiliging en privacy?

Het uitwisselen en verwerken van persoonsgegevens en de middelen waarmee dit gebeurt, worden blootgesteld aan een groot aantal, al dan niet opzettelijke, bedreigingen en risico's. Het kan variëren van een gerichte aanval om gegevens te stelen, of systemen te ontregelen tot een vergissing van een medewerker of een situatie van overmacht. Wanneer dit optreedt kunnen persoonsgegevens kwijtraken en in handen van onbevoegden komen. Als dat gebeurt is er sprake van een beveiligingsincident, dat kan leiden tot een datalek. Dit is een inbreuk op de privacy van degenen op wie de persoonsgegevens betrekking hebben. Naarmate een organisatie meer middelen gebruikt in de uitwisseling en verwerking van persoonsgegeven, wordt de noodzaak om doeltreffende preventieve en reactieve maatregelen te nemen, deze actueel te houden en regelmatig te evalueren, groter. Dit geldt ook voor het SWV.

1.1 Waar richt IBP-beleid zich op?

Informatiebeveiliging is het doorlopende proces voor het beschermen van SWV tegen het risico op het ontstaan van een datalek. Het richt zich op drie aspecten:

- Beschikbaarheid; informatie en aanverwante bedrijfsmiddelen zijn toegankelijk wanneer nodig;
- Integriteit; informatie en verwerkingsmethoden bevatten zo min mogelijk fouten;
- Vertrouwelijkheid; informatie is alleen toegankelijk voor diegenen die daartoe bevoegd zijn.

Als SWV Helmond-Peelland PO beperken we de risico's en de mogelijke persoonlijke, financiële en organisatieschade zoveel mogelijk door de informatie die we in het kader van ons werk gebruiken te beveiligen (informatiebeveiliging) en door verantwoord om te gaan met de persoonsgegevens van onze collega's, kinderen en hun ouders (privacy). In dit stuk beschrijven we hoe we dat samen met alle collega's op hoofdlijnen regelen (hoofdstuk 2) en organiseren (hoofdstuk 3).

1.2 Doel en reikwijdte van IBP

Informatiebeveiliging is een belangrijke voorwaarde voor privacy, terwijl omgekeerd de zorgvuldige omgang met persoonsgegevens noodzakelijk is voor de veiligheid van die informatie. Ze staan naast elkaar en zijn van elkaar afhankelijk en worden daarom samengevoegd tot een proces voor informatiebeveiliging en privacy, afgekort als IBP.

IBP-beleid legt in feite de verbinding tussen de AVG en ICT. Het is erop gericht om de kwaliteit van de informatiebeveiliging en van de verwerking van persoonsgegevens te optimaliseren met als doel:

- de continuïteit van passend onderwijs en de bedrijfsvoering te waarborgen;
- de privacy van alle betrokkenen waarvan SWV Helmond-Peelland PO persoonsgegevens verwerkt te garanderen;
- privacy- en beveiligingsincidenten te voorkomen en de eventuele gevolgen hiervan te beperken.

IBP is van toepassing op:

- het verwerken van persoonsgegevens van in ieder geval alle medewerkers, kinderen, ouders/verzorgers, bezoekers en externe relaties (inhuur/outsourcing), evenals op anderen waarvan we persoonsgegevens verwerken. Hierna noemen we hen betrokkenen.
- al onze (deels) geautomatiseerde systemen en de daarin opgeslagen informatie; dus digitaal zoals in een bestand maar ook op papier;
- al onze apparaten van waaruit geautoriseerde toegang tot het school/organisatienetwerk kan worden verkregen (dus inclusief laptops, printers, telefoons etc.);
- alle applicaties, ofwel software voor eindgebruikers zoals Microsoft Office 365 en KindKans, die we ter beschikking stellen aan medewerkers, inclusief de informatie3 erin.
- al onze samenwerkingen met partners waarbinnen persoonsgegevens worden uitgewisseld, een belangrijk voorbeeld hiervan is de samenwerking met scholen en de Gemeente uitgewerkt in het Privacy Convenant Samenwerking Onderwijs-Gemeenten-Jeugdhulp.

IBP-beleid heeft raakvlakken met:

- Sociale veiligheid en fysieke veiligheid: met als aandachtspunten risicoanalyses en evaluaties, fysieke toegang en beveiliging, crisismanagement, klachtenafhandeling, huisvesting en ongevallen;
- Personeels- en organisatiebeleid: met als aandachtspunten in- en uitstroom van medewerkers, wisselingen in functie, rol of taak, functiescheiding en vertrouwensfuncties;
- ICT-beleid: met als aandachtspunten de aanschaf, inrichting, beheer en gebruik van ICT;
- Medezeggenschap: met als aandachtspunt de rol van ouders/verzorgers en scholen (OPR) en medewerkers (PMR).

Hoofdstuk 2 Informatiebeveiliging en privacy bij SWV Helmond-Peelland PO

Bij SWV Helmond-Peelland PO hanteren we als het om IBP gaat een aantal uitgangspunten en beleidsregels. Deze zijn uitgewerkt in diverse protocollen, procedures en modellen die in de organisatie zijn geïmplementeerd en waarvan een overzicht is te vinden in bijlage 3. Voor de sturing, verantwoording, uitvoering en het toezicht hierop, zijn op diverse organisatieniveaus verantwoordelijkheden toebedeeld. Deze komen in hoofdstuk 3 aan bod.

2.1 Onze uitgangspunten

De basis voor IBP bij SWV Helmond-Peelland PO bestaat uit de volgende uitgangspunten:

- We voldoen aan alle relevante wet- en regelgeving (bijlage 1)
- De directeur-bestuurder zorgt ervoor dat IBP is geregeld, is hierop aanspreekbaar en legt er verantwoording over af.
- SWV Helmond-Peelland PO is volgens de wet verwerkingsverantwoordelijke. Het College van Bestuur is het bevoegd gezag namens SWV Helmond-Peelland PO en is eindverantwoordelijk.
- Het veilig omgaan met informatie en privacybescherming in de dagelijkse praktijk is onze collectieve verantwoordelijkheid, dus van zowel het College van Bestuur als van de medewerkers, ouders/verzorgers, leveranciers van producten en diensten (inclusief inhuur/outsourcing) en van andere externe relaties;
- We handhaven de juiste balans tussen privacy, functionaliteit en veiligheid (proportionaliteit).

2.2 Hoe gaan we te werk?

De beleidsafspraken zijn:

1. Het verwerken van persoonsgegevens is altijd gekoppeld aan een specifiek doel en gebaseerd op een van de wettelijke grondslagen. Daarbij is een goede balans tussen enerzijds het belang van SWV Helmond-Peelland PO om persoonsgegevens te verwerken en anderzijds het belang van de betrokken persoon om vrijelijk eigen keuzes te maken met betrekking tot het gebruik van zijn/haar persoonsgegevens essentieel. Bij alle verwerkingen van persoonsgegevens op basis van toestemming kunnen betrokkenen te allen tijde hun toestemming herzien.

2. Via een privacyverklaring informeert SWV Helmond-Peelland PO alle betrokkenen helder, actief en op hoofdlijnen over de verwerking van hun persoonsgegevens die zowel direct als indirect zijn verkregen. Ook staan hierin hun rechten waaronder o.a. het recht op inzage, correctie en verwijdering.

3. SWV Helmond-Peelland PO legt alle verwerkingen van persoonsgegevens in detail vast in verwerkingsregisters en houdt deze up-to-date. We voldoen hiermee aan de documentatieplicht.

4. SWV Helmond-Peelland PO classificeert informatie (in het verwerkingsregister) en informatiesystemen op basis van de aspecten beschikbaarheid (B), integriteit (I) en vertrouwelijkheid (V) (zie ook 1.1). Deze BIV-classificatie is het uitgangspunt voor de risicoanalyse en de te nemen maatregelen. Daarbij is er een balans tussen de risico's die we willen afdekken, de benodigde investeringen en de te nemen maatregelen.

5. Het College van Bestuur van SWV Helmond-Peelland PO sluit met alle leveranciers van digitale informatiesystemen verwerkersovereenkomsten als zij in opdracht van het College van Bestuur persoonsgegevens verwerken. Soortgelijke afspraken worden ook gemaakt met andere organisaties - ook verwerkingsverantwoordelijken - als er persoonsgegevens worden uitgewisseld.

6. SWV Helmond-Peelland PO kijkt bij wijzigingen in de infrastructuur, bij de aanschaf van nieuwe (informatie)systemen en bij nieuwe samenwerkingen vóóraf naar de impact hiervan op de informatiebeveiliging en de privacy-rechten van de betrokkenen, zo nodig via een data protection impact assessment (DPIA), zodat tijdig de juiste maatregelen genomen kunnen worden. Afspraken hierover worden voor de aanschaf vastgelegd in een verwerkersovereenkomst of een andere onderlinge regeling.

7. SWV Helmond-Peelland PO zorgt voor passende technische (beveiligings-)maatregelen om persoonsgegevens en overige data te beschermen tegen risico's die de voortgang van het uitvoeren van de taken voor het SWV, de privacy en de bedrijfsvoering kunnen verstoren. Afspraken over deze technische maatregelen worden vastgelegd in een bijlage bij de verwerkersovereenkomst en/of in een dienstverleningsovereenkomst/service level agreement (DVO of SLA).

8. SWV Helmond-Peelland PO legt beveiligingsincidenten vast en handelt datalekken af volgens het protocol datalekken. Maatregelen worden genomen en zo nodig wordt er melding gemaakt bij de Autoriteit Persoonsgegevens en eventueel bij de betrokkene(n).

9. IBP-beleid is bij SWV Helmond-Peelland PO een continu proces dat minimaal elke twee jaar geëvalueerd en indien nodig aangepast wordt.

2.3 IBP-organisatie

Zoals bij de uitgangspunten in 2.1 is beschreven, is IBP een gedeelde verantwoordelijkheid. Bij alle processen die zich afspelen in de dagelijkse praktijk van het passend onderwijs spelen privacy en informatieveiligheid een rol. Elke collega moet zich bewust zijn van de risico's en heeft de verantwoordelijkheid de informatieveiligheid en privacy mee te waarborgen.
Een aantal rollen zijn speciaal ingericht ten behoeve van IBP. Die staan hieronder beschreven. In de tabel in bijlage 2 zijn ze verder uitgesplitst.

Dit hoofdstuk beschrijft hoe wij binnen het SWV het IBP-beleid belegd hebben. Er wordt daarbij onderscheid gemaakt tussen drie niveaus:

- Richtinggevend (strategisch)
- Sturend (tactisch)
- Uitvoerend (operationeel)

Voor elk niveau wordt beschreven welke rollen welke verantwoordelijkheden en taken hebben en wat de documenten zijn die daarbij passen.

Richtinggevend

Het College van Bestuur

Het College van Bestuur is eindverantwoordelijk voor IBP en stelt het IBP-beleid en de daarbij behorende maatregelen vast. Voorafgaand worden de ALV en de OPR ter advisering geraadpleegd. Het IBP-beleid wordt vervolgens ter goedkeuring aan de Raad van Toezicht voorgelegd.
Jaarlijks wordt in het bestuursjaarverslag gerapporteerd over de realisatie en evaluatie van het IBP-beleid.

Sturend

Functionaris Gegevensbescherming

De functionaris voor Gegevensbescherming (FG) houdt voor het SWV toezicht op de toepassing en naleving van de AVG. De wettelijke taken en bevoegdheden van de FG geven deze functionaris een onafhankelijke en, waar nodig, een beschermde positie in de organisatie.

IBP coördinator

Binnen het SWV is de Bestuurssecretaresse onder aansturing van de Manager Bedrijfsvoering en kwaliteit aangewezen als IBP coördinator. Dit is een taakgebied, zonder wettelijke basis. De IBP coördinator is verantwoordelijk voor het organiseren en garanderen van privacy binnen een organisatie. De IBP coördinator is nauw betrokken bij de uitvoering van het IBP-beleid binnen SWV. De werkzaamheden van de IBP coördinator worden bewaakt door de FG.

De bijhorende verantwoordelijkheden staan beschreven in bijlage 2.

Medewerkers

Alle medewerkers van SWV hebben een eigen IBP-verantwoordelijkheid in hun dagelijkse werkzaamheden. Het privacyreglement en de geldende afspraken over het werkproces binnen het SWV zijn hiervoor leidend.

Waar nodig ondersteunen wij de medewerkers bij de uitvoering van hun werkzaamheden met documentatie, werkprocesbeschrijvingen, technische en softwarematige bedrijfsmiddelen e.d. De IBP coördinator draagt hier zorg voor.

Wij verwachten van onze medewerkers dat zij actief handelen volgens de uitgangspunten van het IBP-beleid en deze uitgangspunten ook uitdragen naar externe partijen. Wanneer zich situaties voordoen die strijdig zijn met uitgangspunten van het IBP-beleid, wordt ervan uit gegaan dat zij in eerste

instantie afgaan op hun eigen oordeel en oplossend vermogen, bij voorkeur in overleg met een directe collega.
Wanneer een situatie leidt tot een groter risico op een datalek, zullen zij dit onder de aandacht brengen van de IBP coördinator en de Functionaris Gegevensbescherming.

Bijlage 1 Wet- en regelgeving met betrekking tot IBP

SWV Helmond-Peelland PO voldoet met IBP aan alle van toepassing zijnde relevante wet- en regelgeving, waaronder de Wet op het Primair Onderwijs, de Algemene Verordening Gegevensbescherming en de Archiefwet.

Het Normenkader IBP FO is leidend voor de te nemen maatregelen voor beveiliging en privacy. SWV Helmond-Peelland PO hanteert dit normenkader dat gespecificeerd is voor het Funderend Onderwijs (FO, waaronder PO en VO) door het Ministerie van OCW, de PO-raad, VO-raad, Kennisnet en SIVON.

De bepalingen van de meest recente versie van het convenant 'Digitale onderwijsmiddelen en privacy' zijn leidend bij het maken van afspraken met leveranciers (ofwel verwerkers), die in opdracht van de SWV Helmond-Peelland PO persoonsgegevens verwerken. Het ROSA-certificeringsschema is het uitgangspunt voor het onderwijs (gebaseerd op ISO 27001) voor een goede beveiliging van informatie en privacy.

Wettelijke beginselen voor gegevensverwerking
Bij het verwerken van persoonsgegevens zijn de wettelijke beginselen over verwerking persoonsgegevens (artikel 5 AVG) leidend. Deze zijn samengevat in de volgende vijf vuistregels:

1. Doelbepaling en doelbinding
Persoonsgegevens worden alleen gebruikt voor uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Deze doeleinden zijn concreet en voorafgaand aan de verwerking vastgesteld. Persoonsgegevens worden niet verder verwerkt op een manier die onverenigbaar is met de doelen waarvoor ze zijn verkregen.

2. Grondslag
Verwerking van persoonsgegevens is gebaseerd op een van de zes wettelijke grondslagen voor de verwerking, namelijk het hebben van toestemming en/of dat het noodzakelijk is voor het uitvoeren van een overeenkomst, omdat het wettelijk verplicht is, om vitale belangen te beschermen, om een taak van algemeen belang of openbaar gezag uit te oefenen of om een gerechtvaardigd belang te behartigen.

3. Dataminimalisatie
Bij de verwerking van persoonsgegevens blijft de hoeveelheid en het soort gegevens beperkt. Dat wil zeggen dat het type persoonsgegevens redelijkerwijs nodig moet zijn om het doel te bereiken; ze staan in verhouding tot het doel (proportioneel). Het doel kan niet met minder, alternatieve of andere gegevens worden bereikt (subsidiair). Dit betekent ook dat data niet langer wordt bewaard dan noodzakelijk.

4. Transparantie
Aan betrokkenen wordt transparant verantwoording afgelegd over het gebruik van hun persoonsgegevens, en ook over het gevoerde IBP-beleid. Deze informatievoorziening vindt ongevraagd

plaats. Daarnaast hebben betrokkenen recht op verbetering, aanvulling, verwijdering of afscherming van hun persoonsgegevens. Ook kunnen ze zich verzetten tegen het gebruik van hun gegevens.

5. Data-integriteit
Er zijn maatregelen getroffen om te waarborgen dat de te verwerken persoonsgegevens juist en actueel zijn.

Nader uitgewerkt:

Doelbepaling en doelbinding:
a. kinderen
Wij verwerken persoonsgegevens van kinderen alleen om ervoor te kunnen zorgen dat het kind binnen het onderwijs extra ondersteuning krijgt en/of op een zo passend mogelijke onderwijsplek terecht komt.

b. personeel
Wij verwerken de persoonsgegevens van medewerkers alleen ten behoeve van de personeelsadministratie. Daaronder vallen de salarisadministratie, de facturering van dienstverlening, het verzuim- en vervangingsbeleid en de functioneringscyclus.

Grondslag
a. kinderen
Het SWV voert taken uit in het kader van de wetgeving Passend Onderwijs, als onderdeel van de Wet op het Primair Onderwijs. In de wet is vastgelegd dat een samenwerkingsverband besluiten neemt over de toelaatbaarheid van kinderen tot het Gespecialiseerd Onderwijs. Ook is vastgelegd dat het een samenwerkingsverband aan scholen en schoolbesturen middelen kan toewijzen voor kinderen met een extra ondersteuningsbehoefte. Om deze taken te kunnen uitvoeren heeft het SWV de persoonsgegevens van de betreffende kinderen nodig. Voor de wijze van uitvoering van de wettelijke taken zijn regionale afspraken gemaakt met en tussen de aangesloten schoolbesturen. Deze zijn beschreven en vastgelegd het ondersteuningsplan.

b. personeel
Het SWV is werk- en opdrachtgever en voert vanuit die hoedanigheid een personeelsadministratie voor alle medewerkers die in dienst zijn, gedetacheerd zijn of ingehuurd worden.

Dataminimalisatie
a. kinderen
Het SWV verwerkt niet meer persoonsgegevens dan strikt genomen noodzakelijk is voor de uitvoering van haar taken. Dit wordt geborgd door:
- duidelijke afspraken over werkprocessen binnen het SWV
- duidelijke afspraken over uitwisseling van persoonsgegevens met scholen en andere externe partners;
- de inrichting van de ICT-systemen, met name KindKans.

Het SWV bewaart persoonsgegevens niet langer dan strikt genomen noodzakelijk is. Het bijhouden van bewaartermijnen en het verwijderen van persoonsgegevens van kinderen is of via een automatische indicatie geregeld via de software (bijv. KindKans) of via een interne procedure. Hierbij worden de wettelijke termijnen gehanteerd.

b. personeel
Het SWV verwerkt alleen persoonsgegevens van medewerkers die van belang zijn voor uitbetalen van salarissen, het voldoen van facturen, het voeren van verzuim- en vervangingsbeleid en de functioneringscyclus.

Transparantie
Het SWV zorgt ervoor dat betrokkenen tijdig en voldoende geïnformeerd zijn over de wijze waarop hun persoonsgegevens gebruikt en bewaard worden. Deze informatievoorziening vindt ongevraagd plaats. De belangrijkste informatie is te vinden in de privacy verklaringen en deze zijn vrij toegankelijk via de website.

Recht op inzage
Alle betrokkenen hebben recht op inzage in de persoonsgegevens die SWV van hen verwerkt.
a. kinderen
Voor de verwerking van persoonsgegevens van kinderen gebruiken wij KindKans.
Binnen de beveiligde omgeving van KindKans worden aan ouders en kind inzagen in het dossier verstuurd. Mochten ouders en kind ook andere notities over het kind willen inzien, dan kan hiertoe een verzoek worden ingediend bij de Manager Passend Onderwijs van het SWV. De Manager Passend Onderwijs bespreekt het verzoek met de directeur-bestuurder van het SWV en maakt, als het verzoek gehonoreerd wordt, afspraken over de inzage met de aanvrager.

b. personeel
Voor de verwerking van persoonsgegevens van medewerkers wordt gebruik gemaakt van de eigen administratie van SWV, de software applicatie van HR2day, Vervangingsfonds, Participatiefonds en de digitale verzuimmodule van de Arbodienst van Bloeij. Voor inzage in de persoonsgegevens kan een medewerker terecht bij zijn/haar direct leidinggevende.

Het recht om vergeten te worden
Het SWV biedt betrokkenen, in overeenstemming met het recht om vergeten te worden (AVG art. 17), de mogelijkheid om de persoonsgegevens te verbeteren, aan te vullen, te verwijderen of af te schermen. Dit is van toepassing in de volgende gevallen:

- als gegevens feitelijk onjuist zijn;
- als de verwerking onvolledig of 'niet terzake dienend' is;
- als de verwerking op een andere manier in strijd met de wet blijkt.

a. kinderen
Een verzoek tot aanpassing of verwijdering van persoonsgegevens van een kind kan worden ingediend bij de Manager Passend Onderwijs van het SWV. De Manager Passend Onderwijs bespreekt het verzoek

met het College van Bestuur van het SWV en voert, als het verzoek gehonoreerd wordt, de aanpassingen door. De aanvrager wordt hiervan op de hoogte gesteld.

b. personeel

Een medewerker kan een verzoek tot verwijdering of aanpassing van persoonsgegevens indienen bij zijn/haar direct leidinggevende. Deze houdt over het verzoek ruggenspraak met de directeur-bestuurder.

Data-integriteit

Het SWV verwerkt alleen persoonsgegevens die juist en actueel zijn en vanuit betrouwbare bronnen worden aangeleverd.

a. kinderen

Voor de persoonsgegevens van kinderen is dit geborgd via het werken met KindKans. Scholen, kinderen, ouders en andere betrokkenen hebben inzage in de uitgewisselde gegevens en hebben de mogelijkheid om aanvullingen en correcties voor te stellen.

b. medewerkers

De persoonsgegevens van medewerkers worden aangeleverd door de medewerkers zelf. Gegevens uit andere bronnen, zoals adviezen van bedrijfsartsen of bedrijfsmaatschappelijk werkenden, worden ter kennisgeving en inzage altijd naar de betreffende medewerker gestuurd.

Al deze uitgangspunten vormen ook de indicatoren voor de periodieke interne evaluaties van het IBP-beleid en voor audits die door externen uitgevoerd gaan worden.

- Rechten van betrokkenen
- Degenen van wie de persoonsgegevens wordt verwerkt, hebben recht op:
- informatie, om te weten wat er met de gegevens wordt gedaan;
- inzage, om de eigen gegevens in te zien;
- rectificatie, om de verwerkte gegevens te laten wijzigen (corrigeren/aanvullen);
- vergetelheid, om alle of een deel van de gegevens te laten verwijderen (tenzij dat wettelijk niet mag);
- beperking van de verwerking, om tijdelijk geen gegevens te laten verwerken (tenzij dat wettelijk niet mag);
- overdraagbaarheid ("portabiliteit"), om de digitaal opgeslagen gegevens die de betrokkene heeft gegeven te ontvangen in een digitaal bestand of om die over te dragen (aan een andere school);
- verzet, om bezwaar te kunnen maken tegen bepaalde vormen van verwerking;
- geen onderwerping aan geautomatiseerde individuele besluitvorming ("profiling"), ofwel de computer mag geen besluiten nemen.

Bijlage 2 Verdeling verantwoordelijkheden

CvB	College van Bestuur
MB	Manager bedrijfsvoering en kwaliteit
IBP coördinator	Bestuurssecretaresse)
IBP coördinator met externe partijen met specifieke kennisgebieden	IBP coördinator i.s.m. externen
FG	Functionaris persoonsgegevens

Wie	**Verantwoordelijk voor**
CvB	➢ beleidvorming en -evaluatie ➢ maatregelen treffen, protocollen en modellen vaststellen ➢ persoonsgegevens zorgvuldig en rechtmatig verwerken
MB	➢ Organisatie inrichten ➢ persoonsgegevens zorgvuldig en rechtmatig verwerken ➢ beleidsadvisering, -voorbereiding en -implementatie (maatregelen, protocollen, processen etc.) ➢ voorbereiden evaluatie beleid en rapportage ➢ (organisatie) interne kennisuitwisseling, communicatie en bewustwording
IBP coördinator	➢ voorbereiden evaluatie beleid en rapportage ➢ zorgdragen voor uitvoering van DPIA ➢ mede-adviseren bestuur bij datalekken (zie FG) ➢ (organisatie) interne kennisuitwisseling, communicatie en bewustwording ➢ mede-aanspreekpunt bij klachten over privacy (zie FG) ➢ registratie en mede toetsen van verwerkersovereenkomsten (zie FG) ➢ coördinatie verwerkingsregisters ➢ afhandeling beveiligingsincidenten m.b.t. de beschikbaarheid en integriteit
IBP coördinator en externe partijen met specifieke kennisgebieden	➢ advisering over technische beveiligingsmaatregelen ➢ (coördinatie) Classificatie/risicoanalyse en ondersteuning bij DPIA ➢ technische ondersteuning bij beveiligingsincidenten m.b.t. de vertrouwelijkheid (zie FG) ➢ ondersteunen/adviseren bij interne kennisuitwisseling, communicatie en bewustwording

	➢ vertrouwelijke en veilige uitvoering van de processen binnen het functiegebied (P&O, Onderwijskwaliteit, Financiën/Administratie/Inkoop, Huisvesting, ICT, Secretariaat) ➢ l.s.m. IBP coördinator classificatie/risicoanalyse en DPIA ➢ i.s.m. IBP coördinator nadenken over en implementatie en controle van het (juiste) gebruik van protocollen, maatregelen, modellen etc. binnen het eigen functiegebied ➢ i.s.m. IBP coördinator nadenken over en implementatie en controle van het (juiste) gebruik van toegangsrechten/bevoegdheden van gebruikers van netwerken/systemen/applicaties die worden gebruikt binnen het eigen functiegebied ➢ input leveren voor en bijhouden van verwerkingsregisters
FG	➢ toezicht op naleving privacy wetgeving ➢ contactpersoon richting Autoriteit Persoonsgegevens ➢ adviseren/ondersteunen bij ontwikkeling beleid, modellen, protocollen, maatregelen et cetera ➢ advies over en toetsen van verwerkersovereenkomsten ➢ advies over en afhandeling (incl. registratie) van datalekken ➢ mede-aanspreekpunt bij klachten over privacy (zie IBP coördinator) ➢ ondersteunen/adviseren bij interne kennisuitwisseling, communicatie en bewustwording

Bijlage 3 Overzicht modellen, protocollen, procedures

In dit overzicht staan de (model)verklaringen, protocollen en werkwijzen die ter implementatie van de beleidsregels zijn gemaakt. Daarnaast worden alle verwerkingen van persoonsgegevens vastgelegd en upto-date gehouden in verwerkingsregisters (zie ook dit overzicht). Actualisatie en andere wijzigingen in de loop der tijd, worden opgenomen in en gecommuniceerd via de daartoe geëigende kanalen.

	Documenten	**Wat is het?**
1	Verwerkersovereenkomsten of Samenwerkingsovereenkomsten/Convenanten (bijv. via Onderlinge regeling verwerkingsverantwoordelijken) Convenant gegevensdeling	Het College van Bestuur sluit een dergelijke overeenkomst af met opdrachtnemers die persoonsgegevens verwerken waarvoor het College van Bestuur verantwoordelijk is. Hierin wordt uitgesloten dat de opdrachtnemer de gegevens voor een eigen doel verwerkt. Wanneer sprake is van meerdere verwerkingsverantwoordelijken dan wel een gezamenlijkheid van verantwoordelijkheid, dan is sprake van een samenwerkingsovereenkomst of convenant en worden afspraken in een onderlinge regeling verwerkingsverantwoordelijken gemaakt.
2	Protocol datalekken	Hierin staat in het kader van de meldplicht datalekken de procedure die de organisatie volgt wanneer er persoonsgegevens zijn gelekt, kwijtgeraakt, gestolen of op een andere manier in verkeerde handen zijn gekomen.
3	Privacyverklaring kinderen en ouders-verzorgers	Verklaring waarin de school (bij aanmelding van het kind) aangeeft welke persoonsgegevens SWV Helmond Peelland PO verwerkt, waarom en op basis van welke wettelijke grond, met wie de school ze eventueel deelt, hoe ze beveiligd zijn en welke rechten de ouder/verzorger heeft m.b.t. deze gegevens. In een bijlage staan de leveranciers (van digitale leermiddelen) die een rol spelen bij de verwerking van persoonsgegevens van het kind.
4	Privacyverklaring medewerkers	Idem als 5, behalve het leveranciersoverzicht.

5	Privacy Statement – website (model)	Verklaring waarin de school/SWV Helmond Peelland PO de bezoeker van de website informeert over de omgang met via de site verzamelde (persoons)gegevens, over het waarom, over de sitebeveiliging en over de rechten van de bezoeker.
6	Verwerkingsregisters m.b.t. kinderen en medewerkers	Naast de organisatiegegevens en die van de Functionaris Gegevensbescherming staan in dit overzicht m.b.t. de persoonsgegevens die SWV Helmond Peelland PO verwerkt: de doelen en wetsgrond, de categorieën betrokkenen en gegevens, de BIV-classificatie, de bewaartermijn, de ontvangers van de gegevens en de beveiligingsmaatregelen (technisch en organisatorisch).
7	DPIA-aanpak (werken toe naar de uitvoering van een DPIA in 2025).	Een DPIA is een instrument om vooraf de privacy risico's van een gegevensverwerking in kaart te brengen. Er wordt in beschreven welke verwerkingen SWV Helmond Peelland PO wil uitvoeren en wat het doel hiervan is. De organisatie beoordeeld erin of de verwerking wel noodzakelijk is en of de belangen van de verwerkingsverantwoordelijke opwegen tegen de inbreuk op de privacy. Verder staat er een beoordeling van de risico's voor de betrokkene(n) in en beschrijft de organisatie de beoogde maatregelen om die risico's in te perken.