Privacy

Algemene verordening gegevensbescherming (AVG)

Passenderwijs, juni 2023

Passenderwijs dient te voldoen aan de Algemene Verordening Gegevensbescherming (AVG) die per 25 mei 2018 van toepassing is in de gehele Europese Unie (EU).
Het doel van uitwisseling van gegevens is altijd in het belang van het kind waarbij professionals een bewuste, gewogen afweging maken.
Passenderwijs dient passende technische en organisatorische maatregelen te nemen om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen garanderen in redelijkheid een passend beveiligingsniveau gelet op de risico's die verwerking van te beschermen gegevens met zich meebrengt. De maatregelen zijn ook gericht op het voorkomen van onnodige verzameling en verdere verwerking van persoonsgegevens.

Het reglement is verbindend voor alle professionals, werkend in dienst of in opdracht van Passenderwijs. Hierbij wordt concreet gedacht aan het Loket, het Meerpartijenoverleg (MPO), de Centrale Toekenningscommissie (CTC) en het uitvoerende Regioteam van Stichting Passenderwijs.

Privacyreglement Stichting Passenderwijs

Artikel 1 Begripsbepalingen

Dit reglement verstaat onder:	
Verwerker	de natuurlijke persoon of rechtspersoon, overheidsinstantie, dienst of nader orgaan dat persoonsgegevens verwerkt ten behoeve van de verwerkingsverantwoordelijke.
Betrokkene	de persoon op wie een persoonsgegeven betrekking heeft.
Regioteam	alle uitvoerende professionals, werkzaam voor het SWV Passenderwijs.
Meerpartijen overleg (MPO)	overleg waaraan de intern begeleider en Passenderwijs deelnemen. Op verzoek van de school kunnen aanvullende partijen worden uitgenodigd (schoolbegeleider, jeugdverpleegkundige, etc.).
Centrale Toekenningscommissie (CTC)	commissie die toelaatbaarheidsverklaringen en arrangementen extra ondersteuning toekent in opdracht van het SWV.
Persoonsgegevens	gegevens, herleidbaar tot een natuurlijk persoon.
Registratie	het geautomatiseerde systeem dat door het Regioteam wordt aangehouden, waarin persoonsgegevens zijn opgenomen van de personen genoemd in art. 4.
SWV	samenwerkingsverband Passenderwijs, verantwoordelijk bestuur van Stichting Passenderwijs.
Verwerkingsverantwoordelijke	het samenwerkingsverband, dat wil zeggen de rechtspersoon die het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.

Artikel 2 Reikwijdte en doelstelling van het reglement

1. Dit reglement is van toepassing op alle persoonsgegevens van een betrokkene die door of namens Stichting Passenderwijs te Woerden worden verwerkt.
2. Dit reglement heeft tot doel:
   a) vast te stellen van welke personen het SWV persoonsgegevens verwerkt;
   b) te voorkomen dat persoonsgegevens worden verwerkt voor een ander doel dan het doel waarvoor ze zijn verzameld;
   c) de rechten van een betrokkene te waarborgen.
3. Binnen het SWV heeft verwerking van persoonsgegevens specifiek ten doel als bron van informatie te dienen ten behoeve van beantwoording van en/of advisering over de hulpvraag neergelegd door de school, met toestemming van een wettelijk vertegenwoordiger/gezagdragend ouder bij het SWV.
4. In de CTC heeft de verwerking van persoonsgegevens de volgende doelen:
   a) als bron van informatie bij de toekenning van extra ondersteuning;
   b) als informatiebron bij behandeling van bezwaarschriftprocedures door de CTC, ten behoeve van adviseurs die daarbij betrokken worden;
   c) voor het voeren van procedures in geval van bezwaar tegen een besluit van de CTC op een bezwaarschrift en in geval van beroep.

Artikel 3 Toestemming

1. Een wettelijk vertegenwoordiger/gezagdragend ouder dient schriftelijk toestemming te verlenen om gegevens op te vragen bij derden, indien nodig.
2. Voor bespreking van de onderwijsbehoefte van een kind met kernpartners (GGD, Jeugdhulp, Speciaal (Basis) Onderwijs, Schoolbegeleidingsdienst, Leerplicht etc.) is toestemming nodig van een wettelijke vertegenwoordiger/gezagdragend ouder.

3. Wanneer de bespreking van het kind niet binnen redelijke termijn na aanmelding bij het SWV plaatsvindt, dient het SWV opnieuw (schriftelijk) toestemming te vragen om het kind te bespreken.
4. In geval van diagnostisch of psychologisch onderzoek wordt, indien daartoe nog geen toestemming is verleend door de betrokkene(n), een aanvullende toestemmingsverklaring naar ouder(s)/verzorger(s) gestuurd.
5. Het SWV is bevoegd *zonder* toestemming van het kind dan wel diens wettelijk vertegenwoordiger persoonsgegevens betreffende de gezondheid van het kind te verwerken, ten behoeve van:
   a) het verdelen en toewijzen van ondersteuningsmiddelen en voorzieningen aan de scholen;
   b) het beoordelen of kinderen toelaatbaar zijn tot het speciaal (basis) onderwijs op verzoek van het bevoegd gezag van een school waar het kind is aangemeld of ingeschreven;
   c) het adviseren over de ondersteuningsbehoefte van een kind op verzoek van het bevoegd gezag van de school waar het kind is aangemeld of ingeschreven.

Artikel 4 Niet-anonieme casuïstiekbesprekingen

1. Persoonsgegevens worden alleen uitgewisseld als er een gerechtvaardigd doel aanwezig is, gelegen in het belang van het kind. Uitwisseling vindt alleen plaats onder deelnemers die de gegevens nodig hebben voor hun taakuitoefening.
2. Aan het casusoverleg nemen alleen die beroepskrachten deel die een directe behandelrelatie of adviesfunctie hebben met het kind dan wel uit hoofde van een specifieke taak of functie een vast teamlid zijn van het overleg.
3. Deelnemers bespreken de kindgegevens niet met anderen van buiten het SWV zonder toestemming van wettelijk vertegenwoordiger/gezagdragend ouder.
4. Indien de wettelijk vertegenwoordiger/gezagdragend ouder bezwaar maakt tegen bespreking van hun kind, worden hun bezwaren gewogen ten opzichte van het belang van het kind. Indien de conclusie is dat de belangen van het kind zwaarder wegen dan de bezwaren van de wettelijk vertegenwoordiger/gezagdragend ouder, dan worden de bezwaren van laatstgenoemden terzijde geschoven. Maar niet dan nadat de professional zijn voornemen om de bezwaren terzijde te schuiven heeft getoetst aan de hand van het 'juridisch Zwitsers zakmes' (zie bijlage voor toelichting). De professional motiveert en documenteert deze beslissing in het dossier van het kind.

Artikel 5 Verantwoordelijkheid van de bewerker

De bewerker van de registratie is verantwoordelijk voor de verwerking van de registratie overeenkomstig de bepalingen van de AVG. De Verwerkingsverantwoordelijke treft daartoe de nodige voorzieningen, waaronder in elk geval zodanige opslag van gegevens dat deze niet voor onbevoegden toegankelijk zijn.

Artikel 6 Categorieën van personen in de verwerking

In de registratie worden uitsluitend persoonsgegevens opgenomen over:

a) kinderen die voor advisering of ondersteuning door de school worden aangemeld bij het Loket van het SWV.
b) familieleden of andere personen uit de omgeving van deze kinderen, voor zover de gegevens in redelijkheid relevant zijn te achten, voor het beantwoorden van de hulpvraag en/of toekennen van het arrangement.

Artikel 7 Opnemen van gegevens

1. In alle gevallen worden in de registratie uitsluitend persoonsgegevens opgenomen die dienstig zijn ter verwezenlijking van het doel van de verwerking.
2. De Verwerkingsverantwoordelijke doet een mededeling aan de betrokkene(n) dat persoonsgegevens over de aanmelding en ten behoeve van de onderwijszorg worden geregistreerd.

Artikel 8 Soorten van gegevens

De volgende persoonsgegevens kunnen worden verwerkt:

a) NAW-gegevens (van kind en wettelijk vertegenwoordiger), nationaliteit en persoonsgebonden nummer;
b) gegevens betreffende gezondheid of welzijn van het kind voor zover die noodzakelijk zijn voor de ondersteuning;
c) gegevens betreffende de godsdienst of levensovertuiging van het kind voor zover die noodzakelijk zijn voor de ondersteuning;
d) gegevens betreffende de aard en het verloop van het onderwijs en ondersteuning, alsmede de behaalde resultaten;
e) gegevens ten dienste van het toekennen van ondersteuningsmiddelen of voorzieningen;
f) gegevens die de aanleiding voor aanmelding bij het SWV weergeven;
g) gegevens die de aard van de onderwijsbehoefte inzichtelijk maken;
h) gegevens die reeds ondernomen activiteiten van de school ten aanzien van het kind inzichtelijk maken;
i) opgestelde onderwijskundige rapporten en/of ontwikkelingsperspectief van het kind;
j) gegevens die door externe partijen wordt verstrekt en betrekking hebben op de ondersteuningsbehoefte waarmee het kind is aangemeld bij het SWV;
k) andere dan de onder a) t/m j) bedoelde gegevens waarvan de verwerking wordt vereist met het oog op de toepassing van een wettelijke regeling.

Artikel 9 Toegang tot gegevens

1. De Verwerkingsverantwoordelijke kan rechtstreekse toegang verlenen tot de in de verwerking opgenomen persoonsgegevens danwel persoonsgegevens verstrekken aan partijen die recht hebben op informatie m.b.t. het ondersteuningsproces van het kind.
2. De volgende functionarissen hebben rechtstreeks toegang tot de in de verwerking opgenomen persoonsgegevens
   a) de secretariële ondersteuning van het loket en de CTC (de bewerker);
   b) de begeleiders passend onderwijs om ondersteuning te kunnen uitvoeren;
   c) de coördinatoren van het Loket om ondersteuning te kunnen toekennen;
   d) de CTC om extra ondersteuning te kunnen toekennen.
3. De Verwerkingsverantwoordelijke kan eveneens rechtstreekse toegang verlenen tot de in de verwerking opgenomen persoonsgegevens danwel persoonsgegevens verstrekken aan diegene aan wie krachtens wettelijk voorschrift deze toegang dient te worden verleend, echter niet dan na deugdelijke legitimatie door diegene.

Artikel 10 Verstrekking van gegevens

1. De verantwoordelijke voor verwerking verstrekt persoonsgegevens uit de verwerking slechts aan anderen dan de in artikel 9 genoemde personen uitsluitend voor zover:
   a) de verantwoordelijke daartoe op grond van enige wettelijke bepaling verplicht is;
   b) de betrokkene op wie de te verstrekken persoonsgegevens betrekking heeft of diens wettelijk vertegenwoordiger daarin heeft toegestemd.
2. De verantwoordelijke verstrekt persoonsgegevens, bedoeld in artikel 3 van dit reglement, niet aan derden, met uitzondering van het bevoegd gezag van de school waar het desbetreffende kind is aangemeld of ingeschreven.

Artikel 11 Beveiliging van gegevens

1. De Verwerkingsverantwoordelijke draagt zorg voor passende technische en organisatorische maatregelen ter voorkoming van verlies of onrechtmatige verwerking van persoonsgegevens. Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau, gelet op de risico's die de verwerking en de aard van de te beschermen persoonsgegevens met zich meebrengen.

2. Bij elektronische verwerking van gegevens wordt toegang verleend op basis van wachtwoordbeveiliging.
3. Eenieder die betrokken is bij de uitvoering van dit reglement en daarbij de beschikking krijgt over persoonsgegevens is verplicht tot geheimhouding daarvan. Dit geldt niet indien een wettelijk voorschrift tot bekendmaking verplicht.

Artikel 12 Inzagerecht betrokkene

1. Indien een betrokkene of diens wettelijk vertegenwoordiger(s) schriftelijk inzage verzoekt, stelt de coördinator de verzoeker binnen een maand na ontvangst van het schriftelijk verzoek, in de gelegenheid de registratie van de hem betreffende persoonsgegevens in te zien.
2. De coördinator kan weigeren aan het verzoek, bedoeld in het eerste lid, te voldoen, voor zover dit noodzakelijk is op grond van een wettelijk voorschrift of op grond van aanwijzingen gegeven door een daartoe bevoegd overheidsorgaan.

Artikel 13 Correctie van onvolledige of onjuiste gegevens

1. Verzoeken om verbetering, verwijdering of aanvulling van de in de verwerking opgenomen persoonsgegevens, worden schriftelijk ingediend door degene op wie de gegevens betrekking hebben of door zijn gemachtigde.
2. Gemachtigden dienen een schriftelijke machtiging over te leggen.
3. Aan de indiener van het in het eerste lid bedoelde verzoek wordt, na een besluit daartoe door of namens de werkgever van degene die de registratie heeft verricht, binnen een maand na de datum van indiening schriftelijk medegedeeld, of, en zo ja, welke verbetering, verwijdering of aanvulling heeft plaatsgevonden.

Artikel 14 Verzet tegen verwerking van gegevens

1. Wanneer de verwerking van persoonsgegevens plaatsvindt op basis van:
   a) noodzakelijkheid voor een goede vervulling van een door de verantwoordelijke verrichte publiekrechtelijke taak, of
   b) noodzakelijkheid voor een gerechtvaardigd belang van de verantwoordelijke of een derde kan betrokkene dan wel diens wettelijk vertegenwoordiger schriftelijk verzet aantekenen tegen de verwerking van de persoonsgegevens, op basis van zijn bijzonder persoonlijke omstandigheden.
2. De verantwoordelijke dient binnen een maand na ontvangst van het verzet te beoordelen of het verzet terecht is. Is dat het geval, dan dient de verwerking van persoonsgegevens onmiddellijk te worden beëindigd.

Artikel 15 Bewaartermijnen

1. Bewaartermijnen zijn van toepassing op diverse groepen van persoonsgegevens binnen Passenderwijs: personeelsgegevens, leerlinggegevens in online systeem, gegevens leerlingbespreking, ruwe gegevens diagnostiek. De bewaartermijn wordt bepaald volgens wettelijke bepalingen en het principe 'niet langer dan nodig'. De volgende bewaartermijnen zijn vastgesteld:
   a) bewaartermijn van personeelsgegevens in het personeelsdossier van medewerkers bedraagt 2 jaar na het moment van uitdiensttreding;
   b) bewaartermijn gegevens sollicitanten: vernietiging na vervulling vacature;
   c) bewaartermijn van gegevens in Tommy bedraagt 3 jaar na afsluiten van het dossier;
   d) bewaartermijn van ruwe testgegevens en IQ verslagen bedraagt 4 volledige schooljaren na het schooljaar van afname; deze gegevens worden centraal gearchiveerd;
   e) bewaartermijn van een toelaatbaarheidsverklaring en EOB bedraagt 7 jaar na afgifte; deze arrangementen worden gearchiveerd door het secretariaat.

f) Bewaartermijn van vergaderstukken/notulen op de SharePoint bedraagt een planperiode van 4 jaar overeenkomend met het ondersteuningsplan. Voor bestuursbesluiten en notulen geldt een bewaartermijn van 7 jaar vanwege de fiscale en/of financiele grondslag.

2. Voor medewerkers die gebonden zijn aan een beroepscode gelden de bepalingen die zijn opgenomen in deze code alleen indien zij expliciet hebben aangegeven de beroepscode te prefereren boven de regelingen die geldend zijn binnen de organisatie.
3. Het besluit en de uitvoering van verwijdering vindt jaarlijks in september plaats en heeft betrekking op het voorgaande schooljaar.
4. Het dossier van Parantion wordt per augustus 2027 volledig verwijderd, dit is drie jaar na afsluiting van het gebruik van Parantion.

Relevante toelichting op het privacyreglement

Gegevensdeling zonder vooraf informatie te verstrekken aan wettelijke vertegenwoordiger(s)
Er kunnen zich omstandigheden voordoen die het noodzakelijk maken, gezien het belang van het kind, dat zijn situatie wordt besproken zonder dat de wettelijk vertegenwoordiger/ gezagdragend ouder daarover van tevoren is geïnformeerd. Dit geschiedt conform de zorgvuldigheidseisen van 'Afweging 3' uit het 'Instrument samenwerken in de Jeugdketen'. Een instrument voor gegevensuitwisseling van het Ministerie van VWS.
Dit betekent dat de professional een gerechtvaardigd doel moet hebben om niet de wettelijk vertegenwoordiger/gezagdragend ouder van tevoren te informeren. Dat doel moet vervolgens worden getoetst aan het 'juridisch Zwitsers zakmes'

Uitgelicht: **Juridisch Zwitsers zakmes**

Bij het 'juridisch Zwitserszakmes' gaat het om toepassing van eisen van subsidiariteit, proportionaliteit en doelmatigheid:

Subsidiariteit	:	het gaat er om dat het minst ingrijpende actie wordt genomen
Proportionaliteit	:	het gaat er om dat de actie in verhouding staat tot het doel
Doelmatigheid	:	het gaat er om dat de gekozen actie de meest geschikte handelwijze is

Belangrijke regels:

a) Vertel welke gegevens u met wie wilt delen. De AVG bepaalt dat iedereen het recht heeft om te weten wat er waar over hem/haar vast ligt en wat er tussen wie wordt uitgewisseld. Iemand dient altijd geïnformeerd te worden.
b) Vraag alleen toestemming wanneer je 'nee' kunt accepteren.
c) Weeg de bezwaren van ouders af tegen het belang van het kind.
d) De principes van subsidiariteit, proportionaliteit en doelmatigheid spelen hierbij een rol.

Welke onderzoeksgegevens over de leerling mogen scholen delen met het SWV met en zonder toestemming van de ouders? (bron: www.passendonderwijs.nl, website ministerie)
Om te beoordelen welke plek voor een kind het meest passend is, heeft het SWV een aantal gegevens over de leerling nodig. Deze gegevens worden (onder andere) verzameld via onderzoek.

Resultaten van onderzoek welke de school ZONDER TOESTEMMING van ouders mag delen met het samenwerkingsverband
Onderzoek dat door de leraren en intern begeleiders zelf wordt uitgevoerd, zoals lesobservaties en informatie uit het leerlingvolgsysteem.

Resultaten van onderzoek welke de school NIET ZONDER TOESTEMMING van ouders mag delen met het samenwerkingsverband
Onderzoek dat door gedrags- en opvoeddeskundigen (al dan niet in dienst van de school) wordt uitgevoerd, zoals een orthopedagoog of psycholoog. Denk bijvoorbeeld aan het afnemen van een IQ-test bij de leerling.

Aanvullende informatie uitwisseling gegevens (bron: handreiking gegevensuitwisseling, Nederlands Jeugdinstituut, 2016)

- Voor schriftelijke of mondelinge uitwisseling van gegevens gelden dezelfde regels
- Anoniem advies vragen is mogelijk indien casus niet tot de persoon herleidbaar is
- Als toestemming voor uitwisseling van gegevens wordt geweigerd, dan alleen uitwisselen op basis van publiekrechtelijke taak school of gerechtvaardigd belang van school of derde, hierbij hebben ouders het recht bezwaar aan te tekenen
- Levensbedreigende situatie? Gegevensuitwisseling op grond van vitaal belang kind
- Gegevensuitwisseling alleen met die partijen die nodig zijn om het doel van de gegevensuitwisseling te bereiken
- Persoonsgegevens van geheimhouders verkrijgen is alleen mogelijk met toestemming of indien sprake is van 'conflict van plichten' of 'goed hulpverlenerschap'.

Regeling ICT, informatiegebruik en protocol datalekken Stichting Passenderwijs

In het onderwijs wordt steeds vaker locatie onafhankelijk en flexibel gewerkt. Dit brengt nieuwe mogelijkheden maar ook risico's en verplichtingen met zich mee. Passenderwijs is ervoor verantwoordelijk dat de apparaten waarop medewerkers werken professioneel beveiligd zijn. Concreet betekent dit dat ieder apparaat waarop gewerkt wordt voor de organisatie beheerd en beveiligd moet worden. Passenderwijs realiseert dit middels het gebruik van Microsoft Intune, een clouddienst voor het beheren van bedrijfsmobiliteit (Enterprise Mobility Management, EMM) die werknemers in staat stelt om productief te zijn terwijl zakelijke gegevens veilig blijven.

Artikel 1 Begripsbepalingen

In deze regeling wordt verstaan onder:	
organisatie	het geheel van de organisatie, waaronder ook begrepen het bestuur en de medezeggenschapsraad;
directeur-bestuurder	degene belast met de dagelijkse leiding van de organisatie;
medewerker	personeelslid of medewerker die op arbeidsovereenkomst of anderszins betaalde of niet betaalde werkzaamheden voor de organisatie verricht;
ICT-middelen	alle elektronische informatie- en communicatie faciliteiten en ICT-apparatuur, door of namens de organisatie aan medewerkers beschikbaar gesteld, alsmede de privé ICT-middelen indien en voor zover zij gebruikt worden op de werkplek en of voor de uitvoering van de door of namens de directeur-bestuurder opgedragen taken;
ICT-apparatuur	elektronische informatie- en communicatiemiddelen, inclusief alle bijbehorende hard- en software en bestanden;
functionaris gegevensbescherming	door het bestuur aangewezen aanspreekpunt voor gegevensbescherming en verwerking;
Informatie van de organisatie	alle bestanden en informatie van de organisatie door of namens de directeur-bestuurder aan medewerkers beschikbaar gesteld, hieronder begrepen informatie van ketenpartners;
beveiligingsincident	gebeurtenis die een bedreiging vormt of kan vormen voor de vertrouwelijkheid, integriteit of beschikbaarheid van gegevens;
beveiligingsclassificatie	overzicht van de risicoklassen van bestandsgegevens;
privé-bestand	bestand met een geheel of overwegend persoonlijke inhoud;

privé ICT-middelen	ICT apparatuur in eigendom van medewerker zelf of anderszins verkregen, zonder dat deze door of namens de directeur-bestuurder beschikbaar is gesteld;
persoonsgegeven	elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon in de zin van de Wet bescherming persoonsgegevens;
verwerken van persoonsgegevens	elke handeling of geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens;
verkeersgegevens	gegevens die worden verwerkt voor het overbrengen van communicatie over een elektronisch communicatienetwerk of voor de facturering ervan;
bestand	elk gestructureerd geheel van organisatie- of persoonsgegevens, ongeacht of dit geheel van gegevens gecentraliseerd is of verspreid is op een functioneel of geografisch bepaalde wijze, dat volgens bepaalde criteria toegankelijk is en betrekking heeft op verschillende personen of eenheden.

Artikel 2 Reikwijdte

1. Deze regeling is voor alle medewerkers van toepassing op het gebruik van ICT-middelen en informatie van de organisatie, ongeacht de plaats waar dit plaatsvindt en ongeacht het eigendom van de middelen waarmee informatie wordt benaderd.
2. Tevens is deze regeling van toepassing op de wijze waarop controle op dit gebruik plaatsvindt en op het verwerken van persoonsgegevens in dit kader.

Artikel 3 Gebruik van ICT-middelen en informatie van de organisatie

1. Medewerkers gebruiken de ICT-middelen en informatie van de organisatie primair en hoofdzakelijk voor het uitvoeren van de aan hen opgedragen taken, in overeenstemming met wet- en regelgeving en het doel waarvoor de middelen en informatie zijn verstrekt.
2. Het is medewerkers verboden om ICT-middelen van de organisatie aan een ander ter beschikking te stellen. Informatie van de organisatie mag slechts verstrekt worden aan daartoe geautoriseerde anderen.
3. De ICT-middelen en informatie van de organisatie worden beschikbaar gesteld voor zakelijk gebruik. Privégebruik van informatie van de organisatie en bestanden is niet toegestaan.
4. Gebruik van de ICT-middelen of informatie van de organisatie voor commerciële doeleinden is niet toegestaan.
5. Het is medewerkers toegestaan gebruik te maken van privé ICT-middelen voor de uitvoering van de hen opgedragen taken, mits de medewerkers zich hierbij houden aan de bepalingen van deze regeling en bevoegd zijn tot de voor de uitvoering van deze regeling noodzakelijke maatregelen.
6. Het is medewerkers niet toegestaan om de ICT-middelen of informatie van de organisatie te gebruiken voor illegale doeleinden danwel het opvragen, versturen, vastleggen of anderszins verwerken van materiaal of informatie die naar algemeen maatschappelijke opvattingen als lasterlijk, beledigend, aanstootgevend of oneervol wordt beschouwd.
7. Medewerkers dienen de gestelde beveiligingseisen ten aanzien van ICT-middelen en informatie van de organisatie in acht te nemen.
8. Medewerkers dienen schade aan, verlies of diefstal van ICT-middelen of informatie van de organisatie onverwijld bij de directeur-bestuurder te melden.

Artikel 4 Toegang tot en beveiliging van informatie van de organisatie

1. De medewerker verschaft zich uitsluitend toegang tot die gegevens waartoe hij geautoriseerd is.
2. Het is de medewerker verboden om anderen dan daartoe geautoriseerde medewerkers toegang tot informatie van de organisatie te verlenen.
3. De medewerker neemt passende technische en organisatorische maatregelen om informatie van de organisatie te beveiligen tegen verlies of tegen enige vorm van onrechtmatig gebruik. De medewerker houdt hierbij in ieder geval rekening met: de beveiligingsclassificatie (zie bijlage A) van de informatie; de door de organisatie gestelde beveiligingsvoorschriften; aan de werkplek verbonden risico's; het risico door het benaderen van informatie van de organisatie met andere dan door de organisatie verstrekte of goedgekeurde ICT-apparatuur.
4. De medewerker dient geconstateerde of vermoede beveiligingslekken en beveiligingsincidenten te melden bij de functionaris gegevensbescherming.
5. In geval van dringende redenen kan de directeur-bestuur, of bij diens afwezigheid de functionaris gegevensbescherming, dan wel de voorzitter van het bestuur besluiten tot het nemen van noodmaatregelen voor de gegevensverwerking.
6. De medewerker is verplicht advies of ondersteuning van de leidinggevende of de functionaris gegevensbescherming te vragen indien de medewerker onvoldoende in staat is de beveiligingsvoorschriften uit te voeren of te beoordelen.

Artikel *5* Controle

1. Controle door of in opdracht van de directeur-bestuurder op het gebruik van de ICT-middelen en informatie van de organisatie vindt slechts plaats in het kader van de in artikel 7, eerste lid, genoemde doeleinden.
2. Controle ter verkrijging van inzicht in de mate van gebruik van de ICT-middelen en informatie van de organisatie wordt beperkt tot de verkeersgegevens, die betrekking hebben op tijd, hoeveelheid, omvang en dergelijke zodat deze in redelijke verhouding staat tot het doel waarvoor deze wordt aangewend.
3. De controle vindt in beginsel geanonimiseerd en slechts steekproefsgewijs plaats.
4. Controle in het kader van het beheer van de toegang tot de systemen en het beveiligen van het systeem en het netwerk voor het tegengaan van virussen en andere schadelijke programma's vindt op geautomatiseerde wijze plaats.
5. Onrechtmatig gebruik dan wel misbruik van de ICT-middelen en informatie van de organisatie wordt zo veel mogelijk softwarematig onmogelijk gemaakt.
6. Controle beperkt zich tot autorisatie- en verkeersgegevens van het gebruik van de ICT-middelen of informatie van de organisatie, alleen bij zwaarwegende redenen kan er controle op de inhoud plaatsvinden. Privé-bestanden worden hierbij zoveel mogelijk ontzien.
7. De medewerker die voor de uitvoering van de door de directeur-bestuurder opgedragen taken gebruik maakt van privé ICT-middelen is verplicht mee te werken aan eventuele controles volgens dit artikel. Hierbij worden de regels van dit artikel in acht genomen.
8. Indien een medewerker wordt verdacht van het overtreden van deze regeling, kan gedurende een vastgestelde periode gerichte controle plaatsvinden. Deze gerichte controle wordt slechts uitgevoerd nadat de medewerker is ingelicht dat signalen hierover zijn ontvangen en om zijn reactie is gevraagd.
9. Indien geconstateerd wordt dat een medewerker zich niet houdt aan de bepalingen van deze regeling, wordt de betrokken medewerker zo spoedig mogelijk hierop aangesproken door zijn leidinggevende.
10. Het gebruik van ICT-middelen en informatie van de organisatie door bestuursleden, de medezeggenschapsraad en andere medewerkers met een vertrouwensfunctie, is in beginsel uitgesloten van controle. Dit geldt niet voor de controle op de veiligheid van het elektronische verkeer, voor de overzichten als genoemd in het achtste lid en voor informatie die geen verband houdt met genoemde functies of lidmaatschappen.

Artikel 6 Sancties

1. Medewerkers kunnen disciplinair worden bestraft volgens de regels die vastgelegd zijn in de CAO.
2. Vrijwilligers en andere medewerkers die niet onder de CAO vallen, en deze regeling niet naleven, mogen, al dan niet tijdelijk, geen ICT-middelen en informatie van de organisatie gebruiken, onverminderd de bevoegdheid van de directeur-bestuurder de contractuele relatie te beëindigen.

Artikel 7 De verwerking van persoonsgegevens van medewerkers

1. De verwerking van persoonsgegevens inzake het gebruik van ICT-middelen en informatie van de organisatie heeft de volgende doeleinden:
    a) het verkrijgen van inzicht in de aard en mate van het gebruik van de ICT-middelen en informatie van de organisatie;
    b) het voorkomen van onrechtmatig gebruik dan wel misbruik van de ICT-middelen en informatie van de organisatie;
    c) het beveiligen van het systeem en het netwerk;
    d) het beschermen van de privacy van de medewerkers op de werkplek;
    e) het beschermen van de integriteit en goede naam van de organisatie;
    f) het beheer van ICT-middelen en toegang tot informatie van de organisatie;
    g) kostenbeheersing van het gebruik van ICT-middelen.
2. Van medewerkers kunnen de navolgende persoonsgegevens worden verwerkt inzake het gebruik van informatie van de organisatie of ICT-middelen:
    a) geautomatiseerd verkregen logging-gegevens;
    b) naam en zakelijke persoonsgegevens bij incidentmeldingen;
    c) adresgegevens van de externe of mobiele werkplek;
    d) autorisatiegegevens;
    e) informatie over ter beschikking gestelde ICT-middelen en informatie van de organisatie;
    f) informatie over gebruik van ICT-middelen en informatie van de organisatie;
    g) kosten van het gebruik van ICT-middelen.
3. De directeur-bestuurder treft maatregelen zodat verwerking van persoonsgegevens juist en nauwkeurig plaatsvindt.
4. Wat betreft bewaartermijnen wordt verwezen naar artikel 15 van het privacyreglement van Stichting Passenderwijs.

Artikel 8 Rechten van de medewerker

1. De medewerker heeft het recht om een kopie van een overzicht te ontvangen van de hem betreffende persoonsgegevens die worden verwerkt. De medewerker kan daartoe een schriftelijk verzoek indienen bij de directeur-bestuurder.
2. Indien de betreffende persoonsgegevens feitelijk onjuist, voor het doel of de doeleinden van de verwerking onvolledig of niet ter zake dienend zijn, dan wel in strijd met een wettelijk voorschrift worden verwerkt, kan de medewerker de directeur-bestuurder schriftelijk verzoeken deze te verbeteren, aan te vullen, te verwijderen of af te schermen. Het verzoek bevat de aan te brengen wijzigingen.
3. Het bestuur bericht de medewerker binnen vier weken na ontvangst van het in het tweede lid genoemde verzoek schriftelijk of, dan wel in hoeverre, hij daaraan voldoet. Een weigering is met redenen omkleed.
4. De directeur-bestuurder draagt er zorg voor dat een beslissing tot verbetering, aanvulling, verwijdering of afscherming zo spoedig mogelijk wordt uitgevoerd.

Artikel 9 Onvoorziene omstandigheden

In gevallen waarin deze regeling niet voorziet of bij twijfel over de toepasselijkheid van deze regeling, beslist de directeur-bestuurder.

Artikel 10 Openbaarmaking

De directeur-bestuurder stelt de medewerkers die gebruik maken van de ICT- middelen en informatie van de organisatie op de hoogte van deze regeling.

Bijlage A - Uitwerking classificatieniveau data

Classificatieniveau	Vertrouwelijkheid	Waar	Voorbeelden
Geen	Openbaar	Geen restrictie	ondersteuningsplan, nieuwsbrief, website etc.
Laag	Bedrijfsvertrouwelijk	Werk PC, werkarchief, privé PC	algemene vergaderstukken, personeelsbeleid, diverse formats etc.
Midden	Vertrouwelijk	Werk PC, Office 365, Parantion, beveiligde USB-stick verstrekt door de organisatie	algemene registratiegegevens, casuistiekbespreking etc.
Hoog	Geheim	Werk PC, Office 365, Parantion, beveiligde USB-stick verstrekt door de organisatie	dossiergegevens personeel, persoonlijke gegevens ondersteuningstrajecten, loketbesprekingen, groeidocumenten etc.

Beveiligd e-mailen van bijlagen met persoonlijke content

Passenderwijs maakt gebruik van online dossiers om gegevens veilig op te slaan en te delen. Met de leverancier is een verwerkingsovereenkomst afgesloten waarin de veiligheid van gegevens en de verwerking ervan is geregeld.
Voor het versturen van privacygevoelige informatie middels e-mail wordt gebruik gemaakt van Zivver welke wordt beheerd door Emjee ICT diensten. De volgende richtlijn wordt gehanteerd:

Onderwerp	Intern	Extern
Persoonlijke content in mailtekst	Zivver, niveau 2	Zivver, niveau 3 of 2
Persoonlijke content in bijlage	Zivver, niveau 2	Zivver, niveau 3 of 2
Link groeidocument vanuit platform Parantion	Linken worden gedeeld met code; de gebruiker slaat deze op in zijn OneDrive	Linken worden gedeeld met code

Uitgelicht: veiligheidsniveau Zivver

Bij gebruik van Zivver worden de veiligheidsniveau 's als volgt gebruikt:

- Als de mail vertrouwelijke content in tekst of bijlage bevat en het telefoonnummer van de ontvanger beschikbaar is, wordt gewerkt met sms-verificatie (niveau 3).
- Als de mail vertrouwelijke content in tekst of bijlage bevat en het telefoonnummer van de ontvanger niet beschikbaar is, wordt gewerkt met een vaste toegangscode (niveau 2). Als de ontvanger deze code niet heeft, wordt deze als reply op het verzoek van ontvanger gedeeld, daarmee is ook de ontvanger gecheckt. Het versturen van een vaste toegangscode mag ook gebruikt worden, wanneer het gaat om een groepsverzending waarbij telefoonnummers wel bekend zijn.
- In geval de informatie vertrouwelijk is maar de privacy niet schendt (bv. een factuur/beschikking ten behoeve van een specifieke leerling) kan worden volstaan met het verzenden van een toegangscode per mail (niveau 1).

Bewustwording bij bewerking en gebruik van data en gegevens

Procedure meldplicht datalekken
De wetgever eist dat indien sprake is van een datalek[1] waarbij persoonsgegevens zijn gelekt er binnen 72 uur een melding bij de Autoriteit Persoonsgegevens wordt gedaan. Binnen Stichting Passenderwijs geldt de volgende procedure:

1. De betreffende medewerker meldt bij de functionaris gegevensbescherming dat er mogelijk sprake is van een datalek.
2. Aan de hand van de beleidsregels meldplicht datalekken (uitgegeven door Autoriteit Persoonsgegevens) wordt door de functionaris bepaald of sprake is van een datalek welke gemeld dient te worden bij de Autoriteit Persoonsgegevens dan wel betrokkenen.
3. Indien van toepassing, ondersteunt de functionaris de medewerker bij de melding (de medewerker is verantwoordelijk).

Verwerkersovereenkomsten leveranciers
Passenderwijs houdt wettelijk regie over (de bewerking van) persoonsgegevens van leerlingen en medewerkers. Dit mag niet overgelaten worden aan een externe partij. Passenderwijs beslist wat een leverancier wél en niet met de gegevens mag doen. Deze afspraken dienen wettelijk vastgelegd te worden in een verwerkersovereenkomst. Passenderwijs heeft overeenkomsten afgesloten met de volgende partners:

- Groenendijk Onderwijsadministratie (persoonsgegevens medewerkers)
- Parantion (leerling gegevens opgenomen in het groeidocument)
- Emjee ICT diensten
- SO-diensten (Fritz!, De Kleine Prins, PCOU) die ondersteuningstrajecten uitvoeren op basis van vooraf vastgestelde overeenkomsten.
- Onderwijsadvies (schoolbegeleidingsdienst)

Daarnaast wordt gewerkt met Microsoft (Office 365), deze organisatie heeft uitgebreide Voorwaarden Online diensten, waarin de privacy bepalingen zijn geïntegreerd waardoor een specifieke bewerkersovereenkomst niet nodig is. In geval van nieuwe kernpartners zal getoetst worden of een verwerkersovereenkomst wenselijk is.

Toestemming voor gebruik foto's en video's
Indien Passenderwijs foto's of video's van leerlingen of medewerkers wil publiceren, geldt dat betrokkene expliciet heeft aangeven waar wel of geen toestemming voor wordt verleend. Tevens wordt gelaagde toestemming gevraagd. Denk hierbij aan toestemming voor foto's op de website, in de nieuwsbrief of in sociale media.

Waar mag data van de organisatie staan en waar moeten we op letten?
Privacy gevoelige data van Passenderwijs mag alleen in Office 365, Parantion of op een beveiligde usb-stick van Passenderwijs staan. Documenten met classificatie niveau midden en hoog mogen niet op een externe computer aangetroffen worden. Mocht je toch via een externe computer gegevens bewerken dan mag je geen gegevens downloaden en dien je je ervan te verzekeren dat er geen data achterblijft op de pc. Dit geldt ook voor privé-mail of een onbeveiligde usb-stick. De volgende punten zijn van belang:

- Gebruik voor werk gerelateerde zaken alleen het eigen Office 365-(werk)account
- Bewaak zorgvuldig de inlog-informatie
- Vergrendel het werkstation bij het verlaten van de werkplek (windowtoets + L)
- Mocht je gebruik maken van een usb-stick (niet aanbevolen), zorg dat deze beveiligd is met een wachtwoord (sticks worden geleverd door Passenderwijs)
- Wees alert op de vastgestelde termijnen van gegevens (zie art. 15 privacyreglement)
- Print via de mailbox, deel documenten intern, dit is veilig en geniet de voorkeur

[1] Bij een datalek gaat het om toegang tot of vernietiging, wijziging of vrijkomen van persoonsgegevens bij een organisatie zonder dat dit de bedoeling is van de organisatie. Voorbeelden zijn: kwijtraken van een USB-stick, diefstal van laptop of telefoon, verliezen van gegevens op papier etc.

Risico-situaties waarin de medewerker verantwoordelijkheid draagt

- Bij het downloaden van een pdf wordt deze vaak eerst opgeslagen in de map downloads en blijft daar ook staan, bij een privé-computer staan deze gegevens dan op een niet geautoriseerde plek welke door anderen in te zien is.
  Werk dus altijd vanuit jouw eigen account.
- Bij verlies of diefstal van apparatuur of een usb-stick dient altijd melding gedaan te worden bij de functionaris gegevensverwerking zodat een risico-inschatting gemaakt kan worden. Bedenk dat vooral het NIET melden strafbaar is bij een eventuele escalatie.
- Zorg ervoor dat anderen niet onder jouw account kunnen werken (sluit dus altijd af)
- Meldt altijd bij de functionaris gegevensbescherming indien:
  a) privacygevoelige gegevens per abuis naar een verkeerde persoon zijn gemaild
  b) de pc besmet raakt met een virus of ransomware waardoor gegevens in handen kunnen komen van derden

Functionaris Gegevensbescherming (FG)

Passenderwijs heeft een interne toezichthouder op de verwerking van persoonsgegevens aangesteld. Deze functie is als taak opgenomen in de normjaartaak van één van de medewerkers van Stichting Passenderwijs. De FG houdt toezicht op de uitvoering van de algemene verordening gegevensbescherming zoals deze is geïmplementeerd binnen Passenderwijs en is aangemeld bij de Autoriteit Persoonsgegevens
De functionaris kan lid worden van het Nederlands Genootschap van Functionarissen voor de Gegevensbescherming (NGFG).

Taken en bevoegdheden Functionaris Gegevensbescherming

Taken
De FG heeft de volgende taken:

- het houden van toezicht op verwerkingen van persoonsgegevens;
- toezicht op wijzigingen in bestaande verwerkingen en/of het aanleggen van nieuwe verwerkingen met persoonsgegevens binnen Stichting Passenderwijs; geven van (ongevraagd) advies en doen van aanbevelingen over privacy in het algemeen en de toepassing van de AVG;
- overleg met (de contactpersoon van) de Autoriteit Persoonsgegevens;
- organiseren, inrichten en/of onderhouden van het verwerkingsregister (dataregister) met alle verwerkingen persoonsgegevens binnen Stichting Passenderwijs;
- het (laten) afhandelen van klachten inzake privacy;
- overige door directeur-bestuurder van Stichting Passenderwijs aan de FG opgedragen werkzaamheden aangaande privacy.
- het personeel meldt bij de FG alle (nieuwe) verwerkingen van persoonsgegevens alsmede eventuele incidenten met betrekking tot privacy.

Bevoegdheden

- De FG is bevoegd, zo nodig met medeneming van de benodigde apparatuur, elke plaats in de gebouwen op de terreinen die bij Stichting Passenderwijs in gebruik zijn en waar persoonsgegevens worden verwerkt, te betreden.
- De FG is bevoegd inlichtingen te vorderen van een ieder die onder gezag of in opdracht van Stichting Passenderwijs werkzaam is of overeenkomstig voor of namens Stichting Passenderwijs persoonsgegevens verwerkt.
- De FG is bevoegd inzage te vorderen van zakelijke gegevens en bescheiden waarin persoonsgegevens zijn verwerkt.
- De FG is bevoegd van de gegevens en bescheiden kopieën te maken.

- Indien het maken van kopieën niet ter plekke kan gebeuren, is hij bevoegd de gegevens en bescheiden voor de duur van maximaal één werkdag mee te nemen.
- De FG is bevoegd tot het geven van een opdracht tot het aanmaken van een registratie van persoonsgegevens in overeenstemming met de AVG;
- De FG is bevoegd tot vernietiging van persoonsgegevens, waarvan de bewaartermijn is overschreden of indien de gegevensverwerking onrechtmatig is;
- De FG is bevoegd zich te laten vergezellen en bijstaan door personen die daartoe door hem zijn aangewezen.
- De FG maakt van de bevoegdheden als bedoeld in dit artikelen slechts gebruik voor zover dit redelijkerwijs voor de uitoefening van de taak noodzakelijk is.

Weigering

1. Eenieder, die werkzaam is bij en/of in opdracht werkt van de verantwoordelijke, is verplicht aan de FG medewerking te verlenen, die deze redelijkerwijs kan vorderen bij de uitoefening van zijn bevoegdheden.
2. Indien de medewerking aan de uitoefening van de bevoegdheden van de FG zoals bedoeld in artikel 3, wordt geweigerd, kan Stichting Passenderwijs, op een met redenen omkleed verzoek, toestemming verlenen aan de FG de benodigde handelingen zelfstandig uit te voeren in weerwil van de weigering tot medewerking.
3. De directeur-bestuurder van Stichting Passenderwijs wordt zo spoedig mogelijk in kennis gesteld over de uitvoering van het bepaalde in dit artikel.

Geheimhouding

De FG is verplicht tot geheimhouding van al hetgeen hem op grond van deze regeling bekend is geworden, tenzij de betrokkene in bekendmaking toestemt.