3.00 Beleidsplan informatiebeveiliging en privacy SWV ROOS VO

Geactualiseerd 22-12-2023
Vastgesteld door bestuur op 8 januari 2024
Versie 4.0

Inhoudsopgave 3.00 Beleidsplan informatiebeveiliging en privacy

Inleiding

De wet Passend Onderwijs is op 5 november 2012 gepubliceerd (staatsblad 2012 nr 533) en is per 01-08-2014 in werking getreden. Een van de pijlers van het nieuwe stelsel voor passend onderwijs wordt gevormd door de regionale samenwerkingsverbanden passend onderwijs.
Samenwerkingsverbanden passend onderwijs hebben persoonsgegevens van leerlingen nodig om hun taken goed te kunnen uitoefenen. De wet passend onderwijs (artikel 18a lid 13 Wpo, artikel 17a lid 14 Wvo) heeft dit geregeld door onder meer te bepalen dat het samenwerkingsverband bevoegd is om zonder toestemming van de betrokken leerling of diens wettelijk vertegenwoordiger persoonsgegevens te mogen verwerken die nodig zijn voor het vervullen van de wettelijke taak van het samenwerkingsverband.
Dit betekent dat een samenwerkingsverband, net zo als een school, geen meldingsplicht heeft bij de Autoriteit Persoonsgegevens. Het samenwerkingsverband kan persoonsgegevens van leerlingen verwerken met het oog op:

- verdeling ondersteuningsmiddelen/toekennen arrangementen;
- beoordelen toelaatbaarheid;
- adviseren ondersteuningsbehoefte scholen.

De persoonsgegevens zal het samenwerkingsverband ontvangen van de school die een leerling aanmeldt in het kader van een verzoek om extra ondersteuning (voor het toekennen van een ondersteuningsarrangement, voor advies inzake extra ondersteuning of voor het beoordelen van de toelaatbaarheid van een leerling tot het (voortgezet) speciaal onderwijs).
Dit kan een ingeschreven dan wel een aangemelde leerling zijn.
Vervolgens zal het samenwerkingsverband passend onderwijs de ontvangen persoonsgegevens (geheel of gedeeltelijk geautomatiseerd) verwerken. De Algemene Verordening Gegevensbescherming (AVG) is hierop van toepassing.

Voor een deel gaat het bij die gegevensverwerkingen om ‘gewone’ persoonsgegevens, dat wil zeggen gegevens die niet zijn aan te merken als bijzondere persoonsgegevens als bedoeld in de AVG. Te denken valt aan naam, adres en woonplaats en overige contactgegevens van de leerling. Daarnaast gaat het bij de gegevensverwerkingen in het kader van passend onderwijs om zogenaamde ‘bijzondere’ persoonsgegevens, als bedoeld in artikel 9 AVG.

Om persoonsgegevens te mogen verwerken stelt de AVG de eis dat de verwerking gebaseerd dient te zijn op een grondslag als genoemd in artikel 6 AVG.
Die grondslag is voor samenwerkingsverbanden primair gelegen in de wettelijke verplichting om taken uit te voeren ten behoeve van de aangesloten schoolbesturen.
Het gaat wettelijk om 3 taken in dit verband:

- Het toelaatbaar verklaren van leerlingen tot (voortgezet) speciaal onderwijs, het speciaal basisonderwijs en het praktijkonderwijs en het geven van aanwijzingen voor Leerweg ondersteunend onderwijs (LWOO);
- Het geven van adviezen aan de aangesloten scholen over de ondersteuningsbehoefte van leerlingen;
- Het toekenning van middelen voor extra ondersteuning en -voorzieningen aan scholen, ten behoeve van de ondersteuning van leerlingen.

De wetgever geeft voor het vervullen van deze taken in de wet passend onderwijs een wettelijke grondslag aan samenwerkingsverbanden om hiertoe persoonsgegevens te bewerken. Voor bovenstaande drie taken mogen samenwerkingsverbanden en aangesloten scholen/schoolbesturen zonder toestemming van ouders persoonsgegevens uitwisselen. Ouders dienen wel op de hoogte te zijn van het feit dat dit gebeurt en moeten in staat worden gesteld om gegevens in te zien of te

corrigeren. Dit is de verantwoordelijkheid van de school van inschrijving. Aan derden, behalve de bevoegde gezagsorganen van de betrokken scholen, mogen deze gegevens niet worden verstrekt.

De genoemde grondslagen voor samenwerkingsverbanden zijn eveneens van toepassing wanneer het samenwerkingsverband zich bij de uitvoering van zijn taak laat adviseren door deskundigen, bijvoorbeeld een adviescommissie, zorgadviesteam of zorgmakelaar.

Naast deze wettelijke grondslagen formuleert de AVG ook de grondslag dat verwerking rechtmatig is om '**de *vitale belangen'*** van de betrokkene of van een andere natuurlijke persoon te beschermen'. Ook hiervan kan sprake zijn bij passend onderwijs.
Uitwisseling van persoonsgegevens tussen een samenwerkingsverband en een school of een derde partij (bijvoorbeeld een jeugdhulpinstelling) kan nodig zijn om voor de leerling een ononderbroken ontwikkelingsproces te realiseren, om thuiszitten tegen te gaan, etc.

De AVG formuleert ook de grondslag 'nodig in het ***algemeen belang'*** of 'nodig voor een ***gerechtvaardigd belang'***. Samenwerkingsverbanden zullen in het kader van het tegengaan van thuiszitters ook gegevens verwerken op basis van overleg met bijvoorbeeld gemeenten en leerplicht. Dit zal nodig zijn vanwege het algemeen belang dat hiermee is gediend en heeft ook een wettelijke basis omdat samenwerkingsverbanden wettelijk verplicht zijn om de Onderwijsinspectie te informeren over aantallen en duur van thuiszitters.

Samenwerkingsverbanden die persoonsgegevens bewerken voor andere taken dan de drie taken die hierboven zijn genoemd, dienen zich dus te kunnen beroepen op een van de volgende grondslagen van de AVG: 'bescherming vitaal belang betrokkene', 'nodig in het algemeen belang' of 'nodig voor een gerechtvaardigd belang'.

Het samenwerkingsverband is conform de AVG een 'verwerkingsverantwoordelijke' en geen 'verwerker'. Een verwerker is een instantie die ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt. Een administratiekantoor die de personeelsgegevens van het samenwerkingsverband verwerkt, is zo'n verwerker. Hiermee dient het samenwerkingsverband een verwerkersovereenkomst te sluiten.
Een verwerkingsverantwoordelijke is het orgaan die zelf met een bepaald doel en bepaalde middelen persoonsgegevens bewerkt. Het samenwerkingsverband is een orgaan met een wettelijke opdracht waartoe het nodig is om persoonsgegevens te bewerken en daarmee een 'verwerkingsverantwoordelijke'.

Het samenwerkingsverband is in die gevallen de verantwoordelijke in de zin van de AVG.
Zowel scholen als samenwerkingsverbanden moeten bij de uitvoering van passend onderwijs de eisen in acht nemen die de AVG stelt aan het verwerken van persoonsgegevens. Dit betekent, onder meer, dat scholen en samenwerkingsverbanden:

De AVG formuleert een aantal belangrijke principes voor gegevensverwerking:

- Het gebeurt op een wijze die rechtmatig, behoorlijk en transparant is;
- Het gebeurt alleen voor een uitdrukkelijk omschreven en gerechtvaardigd doel (doelbinding);
- Het beperkt zich tot wat noodzakelijk is voor het doel waarvoor het wordt verwerkt (minimale gegevensverwerking);
- Het gaat om juiste en geactualiseerde gegevens met redelijke maatregelen om waar nodig te rectificeren of te wissen (juistheid).

In privacy termen is een samenwerkingsverband een 'verantwoordelijke' en dus zelf verantwoordelijk voor de gegevens van leerlingen. Zodra de school gegevens aanlevert aan het

samenwerkingsverband, is het samenwerkingsverband verantwoordelijk voor privacybescherming. Het samenwerkingsverband is dus geen bewerker van de school, en er wordt daarom ook geen bewerkersovereenkomst afgesloten door de school met het samenwerkingsverband.

Het samenwerkingsverband mag de gegevens van leerlingen niet aan derden verstrekken, met uitzondering van het bevoegd gezag van de school waar de desbetreffende leerling is aangemeld of ingeschreven. Ook bewaart het samenwerkingsverband de gegevens op een plaats die uitsluitend toegankelijk is voor het samenwerkingsverband en deskundigen die adviseren over de toelaatbaarheid. Het samenwerkingsverband bewaart de gegevens tot drie jaar. Het gaat om gevoelige gegevens die goed (digitaal) beveiligd moeten worden.

Ter voorbereiding op de ingangsdatum van de AVG is naast de vaststelling van dit beleidsplan, een privacyreglement, handboek en een protocol datalekken opgesteld, scholing verzorgd en een Privacy Officer benoemd. Voor mei 2018 worden verwerkersovereenkomsten opgesteld en de gedragsregels over het omgaan met ict en persoonsgegevens uitgebreid.

Hoofdstuk 1: Het beleidskader van informatiebeveiliging en privacy

1.1 Het belang

Uitwisselen van bijzondere persoonsgegevens is onderdeel van het dagelijks werk in het samenwerkingsverband. Hierbij hebben we te maken met een groot aantal mogelijke bedreigingen. Alle systemen die we gebruiken en gegevens die we bewaren en verwerken, kunnen worden bedreigd door bijvoorbeeld een aanval, een vergissing of de natuur (zoals een overstroming of brand). Datalekken, incorrecte gegevens of diensten die niet beschikbaar zijn schaden onze bedrijfsvoering en daarmee het vertrouwen. Daarom zijn de continuïteit van onze dienstverlening en privacybescherming van groot belang. Ook treffen we gericht maatregelen om mogelijke risico's tot een aanvaardbaar niveau te reduceren.

Het bestuur doet daarom een beroep op iedereen die betrokken is bij de activiteiten van het samenwerkingsverband, vanuit een gemeenschappelijke visie en wil, de verwerking van (persoons)gegevens correct te laten verlopen.

Dit beleid gaat dieper in op de bescherming van ict en in het bijzonder persoonsgegevens. Het dient als norm en leidraad voor alle informatieverwerking en biedt een uitgangspunt voor audit en controle.

Dit beleidsplan biedt elke belanghebbende – medewerker, klant of leverancier – een inzage in de manier waarop we omgaan met persoonsgegevens.

1.2 Doelen en reikwijdte

Dit beleidsplan heeft als *doelen*:

- Het waarborgen van de continuïteit van de dienstverlening.
- Het beschermen van de privacy van eenieder van wie het samenwerkingsverband persoonsgegevens verwerkt.
- Het voorkomen en zo goed mogelijk afhandelen van incidenten.
- Het minimaliseren van de eventuele gevolgen van incidenten.

Reikwijdte

Dit document is een leidraad voor iedereen die betrokken is bij het samenwerkingsverband Roos VO. Het is van toepassing op onze eigen medewerkers (staf en bpo-ers), tijdelijk personeel en andere personen die een rol spelen -binnen of voor- swv Roos VO. Het is van toepassing op de hele organisatie, waaronder de fysieke locatie, de systemen op interne en externe locaties en gegevensverzamelingen die gebruikt worden. Het swv huurt werkruimte bij het stafbureau van KPO in Roosendaal en maakt gebruik van de ict dienstverlening van Tongerlo (hardware) en KPO (ict-infrastructuur). Derhalve geldt voor het swv zowel het ict- veiligheidsbeleid van sg Tongerlo als van KPO.

1.3 Algemene uitgangspunten

Wij hechten veel belang aan en respecteren de privacy van onze medewerkers en leerlingen/ouders omdat:

- We de menselijke waardigheid respecteren: iedereen heeft het recht om te beschikken over de informatie die over zichzelf gaat.
- Privacy een mensenrecht en een grondrecht is dat moet worden geëerbiedigd.
- De wet verplicht tot privacybescherming: alle swv's horen de wet na te komen.
- Privacy niet respecteren leidt tot onaanvaardbare risico's, imagoschade en mogelijk zelfs tot financiële schade.

De belangrijkste algemene beleidsuitgangspunten van informatiebeveiliging en privacy bij swv Roos VO zijn:

- Informatiebeveiliging en de bescherming van privacy dient te voldoen aan alle relevante wet- en regelgeving.
- Informatiebeveiliging is een lijnverantwoordelijkheid.
- Veilig en betrouwbaar omgaan met informatie is de verantwoordelijkheid van iedereen.
- Er wordt van alle medewerkers, leerlingen, (geregistreerde) bezoekers en externe relaties verwacht dat zij zich 'fatsoenlijk' gedragen met een eigen verantwoordelijkheid.
- Roos VO is als rechtspersoon eigenaar van de informatie die onder haar verantwoordelijkheid wordt gebruikt.
- Roos VO maakt met alle partijen waarmee persoonsgegevens worden uitgewisseld concrete afspraken over informatiebeveiliging en privacy (verwerkersovereenkomsten).
- IBP is een continu proces, waarbij regelmatig (minimaal jaarlijks) wordt geëvalueerd en wordt gekeken of aanpassing gewenst is.
- Er is een balans tussen de risico's van hetgeen we willen beschermen en de benodigde investeringen en maatregelen.
- Er is een balans tussen privacy, functionaliteit/werkbaarheid en veiligheid.
- De informatiebeveiliging dient de volgende aspecten te waarborgen:
    - *Beschikbaarheid* (de mate waarin gegevens of functionaliteit op de juiste momenten beschikbaar zijn)
    - *Integriteit* (de mate waarin gegevens of functionaliteit juist ingevuld zijn of niet aangetast)
    - *Vertrouwelijkheid* (de mate waarin de toegang tot gegevens en functionaliteit beperkt is tot degenen die daartoe bevoegd zijn)

1.4 Organisatie

Deze paragraaf beschrijft hoe IBP binnen Roos VO is georganiseerd. Er wordt daarbij onderscheid gemaakt tussen drie niveaus:

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

Voor elk niveau worden de rollen, verantwoordelijkheden en taken beschreven en de documenten die daarbij passen.
Noot: in 2020 verandert het bestuursmodel van het swv en daarmee ook de inhoud van paragraaf 1.4 en 1.5.

1.4.1 Richtinggevend

<u>Eindverantwoordelijke</u>

Het bestuur van swv Roos VO is eindverantwoordelijk voor IBP en stelt het beleid en de basismaatregelen op het gebied van informatiebeveiliging en privacy vast. De toepassing en werking van het IBP-beleid wordt op basis van regelmatige rapportages geëvalueerd. De inhoudelijke verantwoordelijkheid voor IBP is gemandateerd aan de directeur van Roos VO.

1.4.2 Sturend

<u>De directeur en de Functionaris Gegevensbescherming</u>

De directeur Roos VO en de Functionaris Gegevensbescherming (FG) in samenwerking met de Privacy Officer (PO) geven terugkoppeling en advies aan het bestuur en sturen de medewerkers aan op uitvoerend niveau. De directeur, de FG en de PO moeten:

- Het beleid vertalen naar richtlijnen, procedures, maatregelen en documenten voor het samenwerkingsverband.

- Het aanspreekpunt zijn voor incidenten op het gebied van informatiebeveiliging en privacy.
- De verdere afhandeling van incidenten binnen Roos VO coördineren.

Functionaris Gegevensbescherming
Het samenwerkingsverband is, ondanks dat de schoolbesturen vertegenwoordigd zijn in het samenwerkingsverband, een zelfstandige verwerkingsverantwoordelijke, zodat het bestuur daarvan, net als het bevoegd gezag, een FG moet aanwijzen.

Een FG is een toezichthouder op de verwerking van persoonsgegevens binnen een organisatie. Deze functionaris heeft geen formele sanctiebevoegdheden, maar wel controlebevoegdheden. Hij adviseert het bestuur van het samenwerkingsverband over privacy en houdt toezicht daarop, handelt vragen en klachten over privacy af, ontwikkelt (interne) regelingen rondom privacy en geeft advies over technologie en beveiliging (privacy by design). De FG moet dan ook voldoende kennis van de organisatie en van privacywetgeving hebben, moet betrouwbaar zijn en moet in onafhankelijkheid zijn werkzaamheden kunnen verrichten. De FG heeft dezelfde ontslagbescherming als leden van de MR. Het samenwerkingsverband werkt sinds 1-1-2019 met een externe FG van de CED-groep.

Privacy Officer
Het samenwerkingsverband heeft –naast de aanwijzing van de FG- ook Privacy Officer benoemd. Deze functionaris is het interne aanspreekpunt voor privacy. De specifieke taken van de PO zijn beschreven in paragraaf 2.4.

1.4.3 Uitvoerend

Functioneel beheerder Kindkans
De functioneel beheerder wordt vanuit de directeur voorzien van een ingevuld werkpakket, bestaande uit richtlijnen, procedures en instructies. Op basis hiervan voert hij zijn taken uit.

Medewerker
Alle medewerkers dragen verantwoordelijkheid met betrekking tot informatiebeveiliging in hun dagelijkse werkzaamheden. Deze verantwoordelijkheden zijn beschreven in o.a. de werkprocessen en het ICT beleid. Daarnaast worden medewerkers in hun dagelijkse werkzaamheden, waar nodig, ondersteund met checklists en formulieren.

Medewerkers worden gevraagd om actief betrokken te zijn bij informatiebeveiliging. Dit kan door meldingen te maken van incidenten, het doen van verbetervoorstellen en het uitoefenen van invloed op het beleid.

Leidinggevende
Naleving van het informatiebeveiligingsbeleid is onderdeel van de integrale bedrijfsvoering. Iedere leidinggevende heeft op uitvoerend niveau de taak om:
- Ervoor te zorgen dat zijn medewerkers op de hoogte zijn van het beveiligingsbeleid.
- Toe te zien op de naleving van het IBP-beleid door de medewerkers, waarbij hij/zij zelf een voorbeeldfunctie heeft.
- Periodiek het onderwerp IBP onder de aandacht te brengen in werkoverleggen, beoordelingen etc.
- Als aanspreekpunt beschikbaar te zijn voor alle personeel gerelateerde IBP-onderwerpen.
- De leidinggevende kan in zijn taak ondersteund worden door de Privacy Officer.

Binnen swv Roos VO is de directeur de direct leidinggevende van de directiesecretaresse swv en de senior orthopedagoog. De senior orthopedagoog is direct leidinggevende van de bpo-ers/ab-ers. De andere betrokkenen, zoals de stafmedewerkers financiën en kwaliteitszorg, de aanvragers school en de ondersteuningscoördinatoren hebben hiërarchisch een andere leidinggevende. Wel worden zij ook functioneel aangestuurd door de directeur van het swv.

1.5 Controle en rapportage

De informatiebeveiligings- en privacy afspraken zoals beschreven in dit beleidsplan en onderliggende handboek worden minimaal eenmaal per jaar getoetst en bijgesteld in een bestuursvergadering. Roos VO ziet privacy en informatiebeveiliging als een doorlopend en cyclisch proces. Dat betekent dat het samenwerkingsverband jaarlijks de organisatie als geheel evalueert, controleert en verbetert. Nieuwe ontwikkelingen of incidenten, binnen en buiten het samenwerkingsverband, aanschaf van diensten of bedrijfsmiddelen en grote wijzigingen in de dienstverlening zijn aanleiding tot extra evaluatie, controle en eventuele bijstelling. Het samenwerkingsverband past classificatie, privacy by design, security by design en privacy by default toe om passende maatregelen te kunnen treffen.

1.5.1 Voorlichting en bewustzijn

Beleid en maatregelen zijn niet voldoende om risico's op het terrein van informatiebeveiliging en privacy uit te sluiten. In de praktijk blijkt de mens meestal de belangrijkste speler. Daarom wordt op de scholen en binnen het swv het bewustzijn van de individuele medewerkers voortdurend aangescherpt, zodat de kennis van risico's wordt verhoogd en veilig en verantwoord gedrag wordt aangemoedigd. Onderdeel van het beleid zijn de jaarlijks terugkerende bewustwordingscampagnes voor medewerkers, deelnemers en gasten. Hiertoe is een set aan vragen en casussen ontwikkeld door het team en wordt gebruik gemaakt van de vragenset 'AVG' van de CED groep.
Verhoging van het beveiligingsbewustzijn is een verantwoordelijkheid van de directeur en de PO, met het bestuur als eindverantwoordelijke.

1.5.2 Classificatie en risicoanalyse

Bij het swv heeft alle informatie waarde, daarom worden alle gegevens waarop dit beleid van toepassing is, geclassificeerd. Het niveau van de beveiligingsmaatregelen is afhankelijk van de classificatie. De classificatie van informatie is afhankelijk van de gegevens in het informatiesysteem en wordt bepaald op basis van risicoanalyses. Daarbij zijn beschikbaarheid, integriteit en vertrouwelijkheid de kwaliteitsaspecten die van belang voor de informatievoorziening.

1.5.3 Incidenten en datalekken

Alle incidenten in het kader van privacy en informatiebeveiliging kunnen worden gemeld via meldpuntprivacy@swvroosvo.nl . De afhandeling van deze incidenten loopt volgt een gestructureerd proces, dat ook voorziet in de juiste stappen rondom de meldplicht datalekken.

1.5.4 Controle, naleving en sancties

De naleving bestaat uit algemeen toezicht op de dagelijkse praktijk van het IBP proces. Van belang hierbij is dat iedereen zijn/haar verantwoordelijkheid neemt en de directeur en de Privacy Officer medewerkers aanspreken in geval van tekortkomingen. Binnen swv Roos VO wordt actief aandacht besteed aan IBP bij de aanstelling van nieuwe medewerkers, in de gesprekkencyclus, met een gedragscode en met periodieke bewustwordingscampagnes en scholingen.

Hoofdstuk 2: Wat houdt informatiebeveiliging en privacy in binnen het swv?

2.1 Algemene verordening Gegevensbescherming

Het Europees parlement stemde in 2016 in met de Algemene Verordening Gegevensbescherming (AVG). Deze nieuwe wetgeving sluit aan op de technologische ontwikkelingen en globalisering. Door de AVG zijn persoonsgegevens van alle EU-inwoners straks op dezelfde wijze beschermd, ongeacht of hun gegevens zijn opgeslagen in Europa of - bijvoorbeeld - de Verenigde Staten.
De AVG is een verordening, dit houdt in dat er rechtstreeks verplichtingen worden opgelegd aan degenen die persoonsgegevens verwerken en degene die rechten toekent aan betrokkenen. Dit geldt ook voor scholen.

2.1.1 De rechten van betrokkenen binnen de AVG

In de kern verschilt de WBP uit 2001 niet zoveel met de AVG.
De AVG geeft betrokkenen meer rechten als het gaat om het verwerken van persoonsgegevens. Belangrijke (nieuwe of aangescherpte) rechten zijn*:*

- *Recht op informatie over gegevensverwerkingen:* Het swv moet leerlingen en/of ouders vooraf en in begrijpelijke taal informeren over welke persoonsgegevens het swv verwerkt en met welk doel. Pas als leerling en/of ouders weten wat er met hun gegevens gebeurt, kunnen ze ervoor kiezen om hun rechten ten aanzien van de verwerking van de persoonsgegevens uit te oefenen.
- *Recht op inzage*: Het recht om een afschrift te ontvangen van alle persoonsgegevens die worden verwerkt, het doel waarvoor ze worden verwerkt, de ontvangers van de gegevens en de herkomst van de gegevens.
- *Recht op correctie*: Verbeteren, aanvullen, verwijderen, afschermen of op een andere manier ervoor zorgen dat de onjuiste gegevens niet meer worden gebruikt.
- *Recht van verzet*: Het recht om bezwaar te maken, in verband met de bijzondere persoonlijke omstandigheden van de leerling, tegen een gegevensverwerking als deze gegevensverwerking plaats vindt op grond van een publiekrechtelijke taak of in het kader van een gerechtvaardigd belang van het samenwerkingsverband of een derde. Het swv dient binnen 4 weken na ontvangst van het bezwaar te beoordelen of het verzet terecht is. Als het verzet terecht is moet de verwerking per direct worden stopgezet. Wordt er geen gebruik gemaakt van het recht van verzet, dan mogen de persoonsgegevens worden verwerkt. Dit laatste wordt ook wel instemming genoemd.

Daarnaast legt de AVG meer nadruk op de verantwoordelijkheid van organisaties zelf om de wet na te leven, transparant te zijn over de omgang met persoonsgegevens en om te kunnen aantonen dat zij zich aan de wet houden. Zo moeten scholen en samenwerkingsverbanden:

- *Beter kunnen onderbouwen waarom je persoonsgegevens van leerlingen en ouders wilt verzamelen en verwerken en hoe lang je de gegevens gaat bewaren.*
- *Duidelijke, actieve, specifieke toestemming vragen aan leerlingen/ouders en de verstrekte toestemming ook kunnen aantonen (als de persoonsgegevens worden gedeeld met anderen dan de staf van het swv en de school waar de leerling is aangemeld of ingeschreven).*
- *Risicoanalyses uitvoeren ter stimulering van bewuste omgang met privacy.*
- *Datalekken melden bij de Autoriteit Persoonsgegevens (AP).*

2.1.2 Voorbereidingen voor de AVG

In onderstaand overzicht zijn de belangrijkste eisen vanuit de AVG door Kennisnet en de Autoriteit Persoonsgegevens (AP) vertaald in een aantal aandachtspunten waaraan organisaties blijvende aandacht moeten schenken.

Nummer	Wat	Hoe
1	Bewustwording	De directe en indirecte medewerkers swv (directiesecretaresse, orthopedagogen, bpo-ers, oco's, aanvragers school) informeren over de nieuwe privacyregels en de impact ervan, aandacht voor de ICT vaardigheden van medewerkers
2	Meer en verbeterde rechten betrokkenen	Voorbereiden op de nieuwe rechten (procedure informeren over gegevensverwerkingen inzage, correctie, verwijdering, verzet opstellen)
3	Overzicht verwerkingen (dataregister)	Gegevensverwerkingen in kaart brengen, conform de documentatieplicht (beschrijf welke gegevens met welk doel worden verwerkt, hoe lang deze bewaard worden en met wie ze worden gedeeld)
4	Privacy Impact Assesment (PIA)	Bij nieuwe ontwikkelingen moeten vooraf de privacyrisico's van een gegevensverwerking in kaart gebracht worden, om vervolgens maatregelen te kunnen nemen om risico's te verkleinen
5	Privacy bij design* en privacy bij default**	Al bij het ontwerpen van producten en diensten zorgdragen voor bescherming van persoonsgegevens* en organisatorische maatregelen treffen om te zorgdragen voor dataminimalisatie**
6	Functionaris voor de gegevensbescherming (FG)	Aanstellen FG is voor swv's verplicht. Vanaf 1 januari 2019 wordt gewerkt met een FG van de CED groep
7	Meldplicht datalekken	Alle datalekken moeten gedocumenteerd worden en op basis van deze documentatie stelt de FG vast of een melding noodzakelijk is
8	Verwerkersovereenkomsten	Bij uitbesteding van verwerkingen moeten overeenkomsten worden opgesteld
9	Toestemming	Toestemming moet actief en specifiek gevraagd worden en worden aangetoond

2.2 Informatiebeveiliging en privacy

Informatiebeveiliging is een proces voor het beschermen van swv Roos VO tegen risico's en bedreigingen met betrekking tot informatie en ICT. Het richt zicht 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.

Privacy gaat om de bescherming van persoonsgegevens conform de huidige wet- en regelgeving. Door het goed toepassen van informatiebeveiliging kan aan deze wetgeving worden voldaan. Vooral het aspect vertrouwelijkheid is hiervoor van belang. Binnen swv Roos VO wordt gewerkt met geheimhoudingsverklaringen, volledigheidsverklaringen en een autorisatiebeleid binnen Kindkans, het programma waarin het gehele proces van aanvragen wordt geregistreerd.

2.3 Privacy 2.0

Om persoonsgegevens te mogen verwerken kent de AVG een aantal uitgangspunten. Deze uitgangspunten gelden voor elke organisatie. Samengevat zijn de (herziene) vuistregels:

1. <u>Doelbepaling en doelbinding:</u>

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 wijze die onverenigbaar is met de doelen waarvoor ze zijn verkregen.

2. <u>Grondslag:</u>

Verwerking van persoonsgegevens is gebaseerd op een van de wettelijke grondslagen: Toestemming, overeenkomst, de wet, publiekrechtelijke taak, vitaal belang van de betrokkene en gerechtvaardigd belang.

3. <u>Dataminimalisatie:</u>

Bij de verwerking van persoonsgegevens blijven de hoeveelheid en het soort gegevens beperkt: Het type persoonsgegevens moet redelijkerwijs nodig zijn om het doel te bereiken; de gegevens staan in verhouding tot het doel (= proportioneel). Het doel kan niet met minder, alternatieve of andere gegevens worden bereikt. Dit betekent ook dat data niet langer mag worden bewaard dan noodzakelijk.

4. <u>Transparantie:</u>

Het swv legt aan betrokkenen (leerlingen, hun ouders en medewerkers) op transparante wijze verantwoording af over het gebruik van hun persoonsgegevens, alsmede over het gevoerde IBP-beleid. Deze informatievoorziening vindt ongevraagd plaats. Daarnaast hebben deze betrokkenen recht op verbetering, aanvulling, verwijdering of afscherming van hun persoonsgegevens. Ook kunnen betrokkenen zich verzetten tegen het gebruik van hun gegevens.

5. <u>Data-integriteit:</u>

Er zijn maatregelen getroffen om te waarborgen dat de te verwerken persoonsgegevens juist en actueel zijn.

Persoonsgegevens moeten adequaat worden beveiligd volgens algemeen en breed geaccepteerde beveiligingsnormen.

Bij alle registraties op basis van toestemming, zal het swv aan de betrokkene een eenduidige, zogenaamde ‘opt-out’, procedure worden aangeboden. Dit betekent dat als de wet toestemming vereist, de toestemming niet impliciet wordt aangenomen, maar toestemming actief en specifiek wordt gevraagd. Er wordt dan niet meer gewerkt met meldingen zoals: 'we gaan er van uit dat u toestemming geeft voor het gebruik van... Als u dat niet wilt, moet u ...'.

2.4 Functionaris Gegevensbescherming

De AVG omschrijft de Functionaris Gegevensbescherming als een sleutelfiguur om ervoor te zorgen dat organisaties voldoen aan het nieuwe wettelijk kader. De AVG bevat regels voor zijn aanwijzing, positie en taken. Het doel van deze richtlijnen is het verduidelijken van de relevante voorwaarden van de AVG om verantwoordelijken en verwerkers te helpen aan de wet te voldoen, maar ook om FG’s in hun functie te ondersteunen.

De werkzaamheden van een FG kunnen onder meer zijn:

- toezicht houden;
- inventarisaties van gegevensverwerkingen maken;
- meldingen van gegevensverwerkingen bijhouden;
- vragen en klachten van mensen binnen en buiten de organisatie afhandelen;
- interne regelingen ontwikkelen;
- adviseren over technologie en beveiliging (privacy by design);
- input leveren bij het opstellen of aanpassen van een gedragscode.

Roos VO heeft er voor gekozen om een FG van de CED groep in te huren. Om deze rol op efficiënte wijze te kunnen vervullen is het essentieel dat er een korte ‘lijn’ is tussen de FG en het swv, in de vorm van een contactpersoon die de rol van Privacy Officer vervult.
Binnen Roos VO vervult de beleidsmedewerker kwaliteitszorg van sg Tongerlo de rol van PO. De taken van del PO omvat:

- Incidentafhandeling.
- Intern aanspreekpunt voor incidenten en meldingen datalekken.
- Onderzoeken en voorkomen risico van uitwisseling gegevens.
- uitwerken algemeen beleid naar specifiek beleid.
- Contactpersoon voor de FG-CED groep.
    - Periodiek overleg en afstemming
    - bespreken meldingen beveiligingsincident – (mogelijke) datalekken
    - Doorlopen procedure + contactpersoon met betrekking tot de afhandeling van een incident/datalek
    - Gezamenlijk met FG-CED groep het (verder) creëren van het bewustzijn voor wat betreft privacy bij medewerkers

2.5 Meldplicht datalekken

Op 1 januari 2016 is de Wet meldplicht datalekken ingevoerd. Door deze meldplicht zijn ook samenwerkingsverbanden verplicht melding te maken van ernstige datalekken bij de Autoriteit Persoonsgegevens. Het nalaten van deze melding kan leiden tot een fikse boete.

De meldplicht is alleen van toepassing wanneer persoonsgegevens worden verwerkt, bijvoorbeeld via de mail. Omdat het swv ook gebruik maakt van leveranciers (bijvoorbeeld Driestar Educatief), wordt met deze bewerker(s) aanvullende afspraken over het melden van datalekken gemaakt en vastgelegd in een verwerkersovereenkomst.

Er is sprake van een datalek als er bij een beveiligingsincident persoonsgegevens verloren zijn gegaan, óf waarbij het niet valt uit te sluiten is dat persoonsgegevens verloren zijn gegaan. Er is

persoonlijke informatie ‘gelekt’. Een klassiek voorbeeld van een datalek is een hack waarbij een database met persoonsgegevens is gestolen. Het verliezen van een usb-stick met daarop de adresgegevens van leerlingen, is ook een datalek.

De meldplicht geldt voor de verantwoordelijke voor de persoonsgegevens, dat wil zeggen het bestuur van het swv. Een leverancier is een bewerker voor het samenwerkingsverband. Er kan worden afgesproken dat een bewerker namens de verantwoordelijke de melding doet, maar dat gebeurt altijd onder verantwoordelijkheid van het schoolbestuur. Dat moet wel worden afgesproken, anders zal de verantwoordelijke zelf de melding moeten doen.

Als er een datalek is, moet daar binnen 72 uur na ontdekking van het lek melding van worden gedaan bij de Autoriteit Persoonsgegevens.

2.6 Tool passend onderwijs en privacy

De digitale privacy tool van de VO Raad geeft overzicht en duidelijkheid over wat samenwerkingsverbanden, schoolbesturen en scholen moeten regelen op het gebied van passend onderwijs en privacy. De tool is een vereenvoudigde weergave van de werkelijkheid en geeft aan de hand van processtappen een overzicht van de privacy aspecten en veel gestelde vragen. De tool is te vinden via https://www.vo-raad.nl/werkdocument/tool-passend-onderwijs-en-privacy#!/.