Beleid Privacy

Versie 1.0 05-07-2017

Skipov basisonderwijs
laat talent groeien

Inhoudsopgave

Wijzigingenoverzicht

Versie	Datum	Wijzigingen	Instemming Directie-beraad	Instemming GMR
1.0	05-07-2017	N.v.t.	10-04-2017	Overlegvergadering GMR-RvB 04-07-2017

Inleiding

De huidige informatiemaatschappij biedt de onderwijswereld veel voordelen. Digitalisering ontsluit een schat aan informatie voor eenieder die er belang bij heeft. Skipov kent meerdere belanghebbenden: Skipov als (onderwijs) organisatie, de basisscholen, de leerling/ ouders, de leerkracht/ medewerker en externe partners zoals softwareleveranciers. Met 1 druk op het toetsenbord is binnen een mum van tijd de gewenste informatie beschikbaar. Daarbij is het mogelijk om zonder al te veel moeite de verkregen informatie te bewerken en te verspreiden. Alles kent echter zijn prijs. Als details over persoonsgegevens worden verzameld en het mogelijk is om deze ongelimiteerd te bewerken en te verspreiden, dan komen kwesties als kwaliteit van de informatie, beveiliging van communicatiekanalen, het beschermen van privacy en aansprakelijkheid naar boven drijven. Zonder regie van bovenaf is het vrijwel zeker dat deze kwesties zullen botsen met het grondrecht op bescherming van de persoonlijke levenssfeer die elke burger binnen Europa heeft. Om de werking van dit grondrecht te garanderen is per 1 januari 2016 de Wet Bescherming Persoonsgegevens (Wbp) van kracht geworden die daarna is uitgebreid met de Meldplicht Datalekken. In 2018 wordt de Wbp vervangen door een nieuwe richtlijn: Algemene Verordening Gegevensbescherming (AVG).
Daarom wordt na deze Inleiding met name gesproken over: privacy wetgeving.

De Wbp geeft definities en bepaalt hoe om te gaan met persoonsgegevens, gegevensverwerking en om aantasting van de persoonlijke levenssfeer te voorkomen. Voor dit beleid zijn dan ook de volgende kernbegrippen uit het Wbp van belang:

- Persoonsgegevens.
  Gegevens die feitelijke informatie bevatten die herleidbaar zijn naar de leerling of medewerker, waardoor diens identiteit bekend kan worden;
- Verwerking van persoonsgegevens.
  Elke handeling, zowel digitaal als handmatig, die door of namens Skipov wordt verricht met betrekking tot persoonsgegevens. Verwerken is onder meer: online en offline persoonsgegevens verzamelen, kopiëren, opslaan, verspreiden, publiceren, delen én uitwisselen.
- Verantwoordelijke, Bewerker en Betrokkene.
  Rollen en daaraan verbonden verplichtingen die ervoor moeten zorgen dat de Wbp wordt nageleefd zoals de wet is bedoeld. Hieronder vallen ook het inzage-, correctie- en verbeterrecht voor degenen die een gerechtvaardigd belang hebben en bewaartermijnen.

Een vertaling van deze kernbegrippen binnen Skipov laat het volgende beeld zien: de raad van bestuur dient als verantwoordelijke ervoor te zorgen dat de administratie en organisatie zodanig wordt ingericht, dat bij de verwerking van persoonsgegevens door het stafkantoor, medewerker en externe partners de privacy van de betrokkenen: leerling/ ouder en medewerker, niet wordt geschonden.

In verband met de leesbaarheid van dit beleid wordt tevens verstaan onder:
- ‘ouder’: ouder(s), opvoeder(s), voogd(en) en verzorger(s).
- ‘medewerker’: de leerkracht/ (O)OP, stafmedewerkers, stagiaire(s), Payroll-medewerker en vrijwilliger.
- ‘gegevens’: zowel geautomatiseerde (ICT) als fysieke (papieren) persoonsgegevens.
- ‘privacy wetgeving’: de huidige Wbp en/ of toekomstige (Europese) privacy regelgeving.

Deze opsomming geldt tenzij de tekst er uitdrukkelijk van af wijkt.

Als onderwijsinstelling is het verwerken van persoonsgegevens binnen Skipov nodig. De inzet van externe partners geeft extra ondersteuning of is mogelijk bij wet verplicht. Extra ondersteuning bijvoorbeeld door software leveranciers van digitale educatieve leermiddelen. Bij wet verplicht bijvoorbeeld het registreren van leerlingen bij het ministerie van OCW (DUO). Hierbij moet Skipov rekening houden met een zorgplicht: het bieden van een veilige (digitale) leer- en verblijfsomgeving aan de leerling/ ouder en tevens bescherming van de privacy van de medewerker. Deze zorgplicht bestond al voor de komst van de Wbp. Daarom bestaat binnen Skipov al beleid zoals een Gedragscode Leerlingen/ Ouders en Gedragscode Personeel en sluit Skipov al bewerkersovereenkomsten af met externe partners zoals software leveranciers.

Door de komst van de Wbp heeft Skipov echter besloten om privacy bescherming op bovenschools niveau te trekken, waardoor privacy op dezelfde manier binnen alle basisscholen wordt toegepast. Hierbij vindt Skipov het belangrijk dat draagvlak bestaat over het beleid privacy.
Alleen dan kan daadwerkelijk een hogere graad van bewustwording en daarmee beïnvloeding van gedrag in en om de school worden gerealiseerd. Een goede communicatie is hierbij van groot belang zodat een ieder de kans krijgt te begrijpen wat dit beleid inhoudt en gemotiveerd raakt de inhoud ervan op te volgen.

Dit beleid geeft informatie over:

- het doel en noodzaak van de verwerking persoonsgegevens;
- hoe privacy wordt beschermd en voor hoe lang;
- welke rechten en plichten er bestaan ten aanzien van persoonsgegevens
- contactpersonen en/ of de vindplaats van documenten om actief informatie in te winnen;

Hierbij wordt bestaand beleid zoveel mogelijk gerespecteerd door het binnen dit beleid als integrale tekst op te nemen of ernaar te verwijzen als Bijlage.

De opzet van dit beleid is gebaseerd op de brochure ‘Privacy op school in 10 stappen’ van Kennisnet. De inhoud is gebaseerd op informatie van de overheid (Autoriteit Persoonsbescherming) en de PO-Raad, Verus en Kennisnet.
Met name wordt in dit beleid aangehaakt bij de praktische vertaling van het Wbp voor het onderwijs middels de Modelprivacyreglementen van de PO-Raad/ Verus:

- gegevens personeel voor PO en VO (december 2015); en tevens
- leerling gegevens voor PO en VO (december 2015).

Beide reglementen maken als Bijlage I deel uit van het beleid, met name zal de inhoud doorslaggevend zijn in situaties dat onduidelijkheid bestaat over de uitleg van dit beleid en/ of het beleid er niet in voorziet.

1 ICT

In de praktijk wordt de verantwoordelijkheid voor het houden van toezicht op de privacy bescherming bij de verwerking van persoonsgegevens uitgevoerd door de afdeling ICT omdat deze de ICT infrastructuur faciliteert en beheert. De infrastructuur bestaat uit een bundeling van netwerksystemen, hardware en software die voor verschillende doelen worden ingezet. Deze doelen worden bepaald door degenen die ermee werken zoals de leerling/ ouder en leerkrachten van Skipov maar ook door stafmedewerkers van Skipov en externe partners zoals de educatieve software leveranciers.

Afhankelijk van het doel en de toepassing hebben bepaalde handelingen betrekking op persoonsgegevens. Te denken valt aan het online en offline verzamelen en uitwisselen van persoonsgegevens, kopiëren, opslaan, verspreiden en publiceren. In principe vallen hier zowel de geautomatiseerde als de handmatige gegevensverwerking onder.
In alle gevallen is sprake van verwerking in de zin van de privacy wetgeving. Besef dat verwerking ruim wordt uitgelegd is belangrijk omdat verwerking een speerpunt is binnen de huidige en nieuwe regelgeving.

Dit blijkt onder andere uit nieuwe Europese regelgeving die de taak datacontroller in het leven roept. Binnen Skipov krijgt de systeembeheerder van de afdeling ICT deze taak die onder andere inhoudt:

- het monitoren en, indien nodig, het treffen van maatregelen bij de verwerking van persoonsgegevens en de eraan verbonden privacy risico's;
- het bijhouden van een database zodat desgewenst informatie kan worden verstrekt aan instanties zoals de Autoriteit Persoonsgegevens hoe binnen Skipov met privacy (bescherming) wordt omgegaan;
- eerste aanspreekpunt op het gebied van Privacy, zowel binnen als buiten Skipov. Dit is vooral van belang ten aanzien van de Autoriteit Persoonsgegevens en Melding Datalekken.

In deze paragraaf ligt het accent op de ICT infrastructuur, de algemene risico's en de veiligheidsmaatregelen die Skipov neemt ten aanzien van de gegevensverwerking. In de paragrafen Leerling/ Ouder en Medewerker, die hierna volgen wordt met betrekking tot de verwerking van persoonsgegevens ingegaan op het specifieke doel, toepassing, risico, bewaartermijn en privacy bescherming.

1.1 Doel op het gebied van de ICT infrastructuur

De privacy wetgeving vereist dat Skipov bij de bewerking van persoonsgegevens zoveel mogelijk de privacy beschermt. Dit geldt in principe alleen voor persoonsgegevens die herleidbaar zijn tot een natuurlijk (rechts)persoon.
Dit is het kader waarbinnen Skipov de beveiliging van de verwerking van persoonsgegevens regelt. Het begrip beveiliging betekent hetzelfde als bescherming en moet ruim worden opgevat. Hieronder valt het initiëren en het beheren van passende technische en organisatorische (veiligheids)maatregelen ter voorkoming van verlies of onrechtmatige verwerking van persoonsgegevens.

Doordat de privacy wetgeving steeds meer wordt aangescherpt, heeft Skipov een risico inventarisatie gedaan met betrekking tot de bestaande ICT infrastructuur en de beveiliging. Doel is het verkrijgen van inzicht met betrekking tot welke hardware en software binnen Skipov wordt gebruikt, hoe persoonsgegevens worden verwerkt en de mate van privacy gevoeligheid.

Binnen Skipov wordt de mate van privacy gevoeligheid aangegeven met de classificatie die de systeembeheerder afgeeft, te weten: laag, midden of hoog. Hierbij wordt rekening gehouden met factoren die invloed hebben op de verwerking van persoonsgegevens:

- functionaliteit: volledigheid, real-time, rapportages;
- gebruikersgroep: leerling/ ouder, medewerkers, externe partners zoals overheid en software leveranciers;
- kwetsbaarheid van de ICT-infrastructuur: website, email, Office365, servers, datadragers,…
- brute force: inbraak, phishing, hacken, malware, ongeoorloofd gebruik.

Het aantal en de invloed van deze factoren bepaalt de classificatie waardoor ook duidelijk is wat de minimumeis aan privacy bescherming is. De afdeling ICT regelt dat de ICT infrastructuur hierop wordt aangepast. De effectiviteit van privacy bescherming is echter altijd mede-afhankelijk van degene(n) die betrokken is (zijn) bij de verwerking van persoonsgegevens.

In deze paragraaf ICT wordt de uitkomst van de risico inventarisatie met betrekking tot applicaties vermeld. Het gaat hier puur om het operationeel zijn van de applicatie binnen de ICT infrastructuur en niet om het feitelijk gebruik, doel en noodzaak. Deze kwesties komen verderop in de beleid aan de orde in respectievelijk de paragrafen Leerling/ Ouder en Medewerker.

1.2 ICT-infrastructuur

Op het moment dat leerlingen/ ouders en medewerkers worden aangemeld (of afgemeld) bij Skipov, vindt registratie plaats in de zogenaamde active directory. Deze active directory is een real time verzamelbestand waarbinnen elk persoon een status en daaraan verbonden gebruikersrechten verkrijgt (of verliest) om te kunnen werken binnen de ICT infrastructuur van Skipov. Te denken valt aan (de informatiepleinen van) SharePoint. Dit hele proces wordt binnen Skipov geregeld aan de hand van het Role Based Access Control (RBAC) model. Dit model houdt in dat de betrokken persoon een ICT-rol wordt toegekend (of afgenomen). Vervolgens worden aan de ICT-rol bepaalde gebruikersrechten en mate van toegang gekoppeld. Deze informatie is versleuteld in het Skipov account en het wachtwoord wat de leerling/ ouder of medewerker ontvangt. Inloggen leidt ertoe dat automatisch authenticatie en autorisatie toegang tot bepaalde afgeschermde persoonsgegevens wordt verleend (of geweigerd).

Daarnaast probeert Skipov zoveel mogelijk het Single Sign On (SSO) met de leverancier af te spreken als in een beveiligde omgeving wordt gewerkt die buiten de ICT infrastructuur van Skipov valt. Te denken valt aan het leerlingvolg- en administratie systeem van ParnasSys. Toegang tot deze externe omgeving is geregeld via het eenmalig inloggen met het eigen Skipov account en wachtwoord.

In het algemeen geldt dat als de medewerker uitdienst gaat of de leerling/ ouder Skipov verlaat, de ICT-rol van deze persoon uit het active directory wordt gehaald. Hierdoor wordt de keten van authenticatie en autorisatie direct doorbroken en de toegang per direct wordt geweigerd.

Binnen Skipov is dit beschreven in een 2-tal processen: het Back-up en recovery proces en een Autorisatie en authenticatie proces.

1.3 Gebruik (hardware en) software

Automatisch worden alle gegevens gewist nadat gebruik van hardware is beëindigd. Tevens vindt er elke dag back-up plaats van persoonlijke en/ of gedeelde bestanden. Daarnaast wordt een uitdrukkelijk beroep gedaan op de gebruiker zelf door de Gedragscode Leerling/ Ouder en Gedragscode Personeel.
De integriteit van de informatie valt en staat immers met het gebruik van hardware en software.
Intern hanteert Skipov Gedragscodes en Handleidingen om de omgang met en de kwaliteit van de informatie zo goed mogelijk te bewaken. Extern sluit Skipov Bewerkersovereenkomsten af met externe partners waarbij, in zoverre beschikbaar, de Digitale Bijsluiter Privacy wordt gecheckt.
Meer informatie over het gebruik van hardware en software staat vermeld op SharePoint, Startpagina: Handleidingen.

1.4 Firewall

Skipov maakt gebruik van een Professional Enterprise Solution waardoor Brute Force en andere aanvallen van buitenaf tot een minimum wordt beperkt.

1.5 Gedragscodes en Handleidingen

Informatiebeveiliging is niet af te dwingen met technische of organisatorische maatregelen alleen. Betrokkenheid en verantwoordelijkheidsgevoel van de leerlingen/ ouders en medewerkers is essentieel. De Gedragscode Leerling/ Ouder en de Gedragscode Personeel worden bij aanmelding en tewerkstelling schriftelijk onder de aandacht gebracht en zijn gepubliceerd op de school website en op SharePoint, Skipov handboek, Codes en Protocollen.

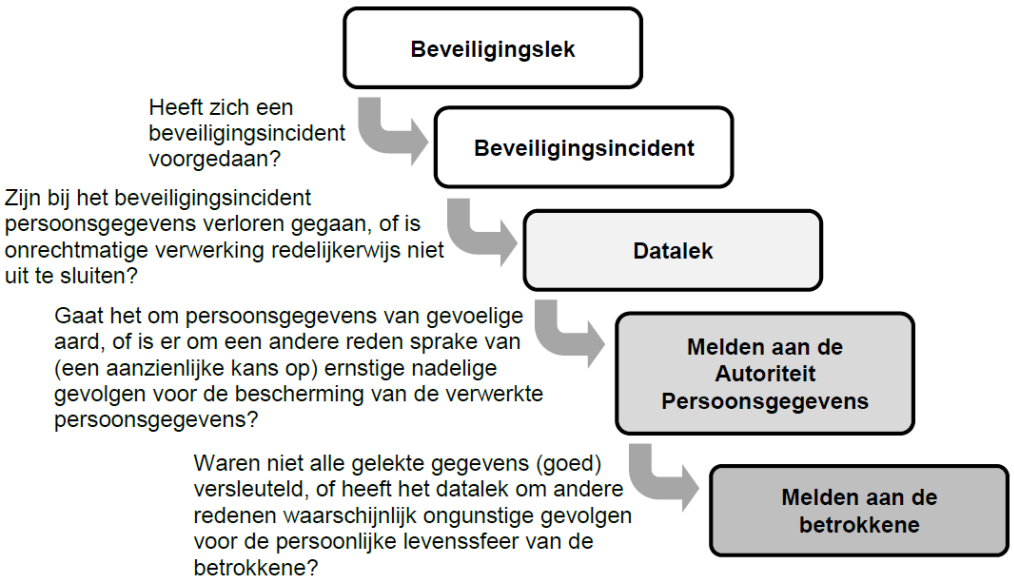
1.6 Externe partners

Skipov sluit SLA/ Modelbewerkersovereenkomst met externe partners af zoals met name software leveranciers. Daarbij wordt tevens, indien aanwezig, de Digitale Bijsluiter Privacy gescreend. Het belang voor Skipov is dat de software leverancier ervoor in staat te voldoen aan de eisen die de Wbp stelt. De overeenkomsten gaan over het implementeren van systemen met betrekking tot de salaris en personeelsadministratie, educatieve software, digibord en over het leerlingadministratie- en volgsysteem. Skipov gebruikt de modelovereenkomsten die de PO-Raad heeft opgesteld voor de onderwijssector.

1.7 Meldplicht Datalekken

Skipov probeert zoveel mogelijk te voorkomen dat de Meldplicht van toepassing is. Dit valt en staat met de beveiliging van de privacy bij de verwerking van persoonsgegevens, kortgezegd: het waarborgen van vertrouwelijkheid. Binnen Skipov wordt vertrouwelijkheid zoveel mogelijk gegarandeerd door de toegang tot persoonsgegevens en de bevoegdheid deze te bewerken te koppelen aan een active directory en de ICT-rol. Meer details staan hierboven onder het kopje ICT-infrastructuur.

Skipov houdt zich aan de Meldplicht zoals het proces op de website van de Autoriteit Persoonsgegevens aangeeft. Zoals aan het begin van deze paragraaf is aangegeven, voert de systeembeheerder binnen Skipov de taak van datacontroller uit. Hierdoor is hij degene die de Meldplicht Datalekken namens Skipov zal doen. Het volgende stroomschema van de Autoriteit Persoonsgegevens laat zien dat lang niet elke datalek gemeld hoeft te worden:



2 Leerlinggegevens in de school

Op grond van het GMR reglement heeft de oudergeleding van de GMR instemmingsrecht met betrekking tot de verwerking van persoonsgegevens van de leerling en de ouder. Deze paragraaf vermeldt voor de leesbaarheid ouder of leerling(gegevens). Mogelijk worden echter beiden bedoeld omdat de privacywetgeving bepaalt dat de leerling van de basisschool door de ouder(s) wordt vertegenwoordigd. Voor de precieze reikwijdte van het begrip ouder(s) wordt verwezen naar de Inleiding van dit beleid. In geval de ouders uit elkaar gaan wordt binnen Skipov het Scheidingsprotocol gevolgd.

Als wordt gesproken over de verwerking van persoonsgegevens van de leerling wordt alles bedoeld wat er onder zou kunnen vallen, zoals het online en offline verzamelen van persoonsgegevens, kopiëren, opslaan, verspreiden, publiceren, delen én het (onderling) uitwisselen. Dit slaat niet alleen op feitelijke informatie, maar ook op foto's, video's en dergelijke. Alles wat hierbij herleidbaar is tot de individuele leerling valt onder de privacybescherming. Binnen Skipov wordt hierbij geen onderscheid gemaakt tussen geautomatiseerde en handmatige gegevens(verwerking).

In deze paragraaf wordt ingegaan hoe binnen Skipov wordt omgegaan met leerling gegevens, op de inhoud van het leerling dossier, het doel en de verwerking van leerling gegevens en de maatregelen die genomen worden ten aanzien van de privacy risico's.

2.1 Doel

Bij de aanmelding van een leerling bij een basisschool van Skipov start de verwerking van leerling gegevens. De basisschool stuurt op grond van het Toelatingsbeleid de ouder(s) informatie toe en vraagt daarnaast de ouder(s) informatie te verstrekken. Het Toelatingsbeleid houdt rekening met ontwikkelingen zoals bijvoorbeeld ten aanzien van het BSN/ BRIN-nummer, kopie ID-bewijs en foto/ video gebruik. Daarbij wordt een Toestemmingsformulier aan de ouder(s) verstrekt waarin de specifieke doelen voor de verwerking van leerling gegevens staat uitgelegd en akkoord/ toestemming wordt gevraagd. Te denken valt aan het gebruik van foto en video. Op het Toestemmingsformulier staat ook uitdrukkelijk aangegeven dat een gegeven akkoord/ toestemming gewijzigd kan worden.

Het komt natuurlijk voor dat na de aanmelding bij een basisschool nieuwe redenen ontstaan voor het verwerken van leerling gegevens. Dit wordt mogelijk veroorzaakt door externe factoren. Dan gaat het met name om ad hoc verzoeken van instanties zoals de gemeente en GGD. In al deze situaties beoordeelt de schooldirecteur of specifiek toestemming/ akkoord van de ouder(s) gevraagd zal worden.

Bij dit alles is Skipov zich ervan bewust dat sprake kan zijn van bijzondere of gevoelige persoonsgegevens. Dit zijn persoonsgegevens van de leerling die extra gevoelige informatie bevatten, zoals bijvoorbeeld gezondheid, gedragsproblemen, godsdienst of een problematische thuissituatie. Deze gegevens worden alleen vastgelegd en verwerkt als dit noodzakelijk is voor het doel zoals bijvoorbeeld speciale begeleiding gedurende het schooltraject of het treffen van bijzondere voorzieningen zodat in geval van nood de juiste procedure kan worden gevolgd.
Bij dit laatste valt te denken aan bijvoorbeeld een leerling met epilepsie of bepaalde allergieën. Meer details staan in het Medisch Handelingsprotocol.

Vanaf de inschrijving is het de ouder(s) duidelijk dat alle leerling gegevens worden verzameld in het leerling dossier totdat de leerling (tussentijds) vertrekt bij een basisschool van Skipov. De verantwoordelijkheid voor een correcte en datalek-vrije overdracht van het leerling dossier ligt bij Skipov. Deze overdracht gebeurt via de overstapservice Onderwijs (OSO) waardoor de privacybescherming bij het overhevelen van de informatie optimaal is. Nadat een leerling is uitgeschreven en het leerling dossier is overgedragen, wordt het leerlingdossier nog 5 jaar bewaard, conform paragraaf 2.3.3.

2.2 Onze vooraf gestelde doelen met de verwerking van leerling gegevens

Als onderwijsorganisatie heeft Skipov de volgende doelen bij de verwerking van leerling gegevens:

- Het organiseren en het geven van onderwijs;
- Het begeleiden van leerlingen op het juiste niveau;
- Het gebruik van educatieve software en digibord;
- Het publiceren van informatie ten behoeve van zowel de leerling als de groep;
- Het berekenen, vastleggen en innen van bijdragen en vergoedingen zoals bijvoorbeeld de ouderbijdrage;
- Gebruik van de leerling volg- en administratiesysteem;
- De communicatie met de leerling, met de ouder(s), instanties;
- Verslaglegging van leerling gerelateerde dingen zoals onderzoek, gesprek, behandeltraject;
- Het voldoen aan wettelijke verplichtingen van (vertegenwoordigers van) overheidsinstanties zoals de Onderwijs Inspectie, belastingdienst, DUO, stichting CITO, Veilig Thuis, het 30.06 Samenwerkingsverband en de gemeente met betrekking tot leerplicht.

Alle gegevens die te maken hebben met een van bovenstaande doelen en relevant zijn voor de individuele leerling worden, zoals hierboven al aangegeven, verzameld in een leerling dossier zolang de leerling op een basisschool van Skipov staat ingeschreven.

2.3 Het leerling dossier

Skipov gebruikt de benadering die binnen het onderwijs geldt met betrekking tot de opbouw van het leerling dossier. Dit houdt in dat binnen Skipov het leerling dossier bestaat uit de leerling administratie en gegevens die te maken hebben met het leerling volg –en leerproces. Hier valt een onderwijskundig rapport ook onder.

Het leerling dossier vormt binnen Skipov de basis voor het verwerken van leerling gegevens zoals het opslaan en bijhouden van feitelijke persoonsgegevens en de leer- en begeleidingsgegevens. Hierbij houdt Skipov rekening met de rechten van de leerling met betrekking tot het leerling dossier. Deze rechten worden door elk van de ouder(s) uitgeoefend als wettelijk vertegenwoordiger(s) van de leerling. Dit kan veranderen als een van de ouders het ouderlijk gezag, de voogdij krijgt zoals bijvoorbeeld door een scheiding. Gedragscodes zoals het Scheidingsprotocol van Skipov bepalen hoe per situatie met de rechten van de ouder(s) wordt omgegaan.

2.3.1 Inzagerecht en andere rechten van de ouder(s)

Ten aanzien van het leerling dossier heeft in principe elke ouder een:

- Inzagerecht.
    - De basisschool binnen Skipov bepaalt welke digitale gegevens uit het leerling dossier voor de ouder(s) toegankelijk zijn via het Ouderportaal van ParnasSys.
    - Als ouders het leerlingdossier willen inzien, kan een afspraak met de schooldirecteur worden gemaakt.
    - Informele documenten zoals notities die een persoonlijke mening weergeven en die slechts bedoeld zijn voor intern overleg mogen van inzage worden uitgesloten.
- Kopierecht.
  Op verzoek van de ouder(s) verstrekt Skipov een kopie van het leerling dossier tenzij het dossier te omvangrijk is. In dat geval vraagt Skipov specifiek aan te geven van welke documenten een kopie wordt gewenst. De wachttijd voor de kopie is maximaal 4 kalenderweken.
- Correctierecht met betrekking tot strikt feitelijke persoonsgegevens.
  Het staat de ouder(s) vrij om een schriftelijk verzoek bij de schooldirecteur van de betreffende basisschool in te dienen om bepaalde leerling gegevens te corrigeren. Dit correctierecht heeft betrekking op het verbeteren, aanvullen, verwijderen, afschermen en weghalen van leerling gegevens, omdat deze naar de mening van de ouder(s) bijvoorbeeld niet relevant zijn en/ of sprake is van onjuistheid of onvolledigheid. De schooldirecteur neemt contact op om een correctieverzoek door te spreken en legt uit wat de uiteindelijke beslissing is. Ten aanzien van het onderwijskundig rapport geldt echter dat alleen een verzoek om aanvulling is toegestaan.
- Klachtrecht.
  Bij ontevredenheid van de ouder(s) over de inhoud of het proces van de basisschool ten aanzien van het leerling dossier, vindt eerst een gesprek plaats met de schooldirecteur. Als dit op niets uitdraait, kan de klachtenregeling van Skipov gevolgd worden.

Het correctierecht is beperkt tot strikt feitelijke persoonsgegevens. Persoonsgegevens die niet helemaal feitelijk zijn zoals een voor de leerling nadelige beoordeling of inschatting, vallen dus niet onder het correctierecht. Het kan immers niet zo zijn dat een ouder ‘’alles wat ongewenst is’’ uit het leerlingdossier kan krijgen. Skipov zal in zo’n situatie na goed overleg het standpunt van de ouder(s) opnemen in het leerlingdossier.

2.3.2 Inzagerecht door anderen

In bepaalde gevallen is Skipov wettelijk verplicht om informatie over de leerling aan bepaalde instanties te geven. Die informatie beperkt zich tot wat relevant is. Hierdoor is het niet nodig vooraf toestemming van de ouder(s) te vragen. Te denken valt bijvoorbeeld aan:

- Informatieverstrekking bij de doorverwijzing naar het speciaal basisonderwijs;
- Informatieverstrekking bij (tussentijds) vertrek van de basisschool;
- Noodsituaties die onmiddellijke behandeling vereisen door bijvoorbeeld een dokter of tandarts;
- Vermoedens van kindermishandeling, leerplichtverzuim en andere situaties die het welzijn en de gezondheid van de leerling bedreigen;

2.3.3 Bewaartermijn leerling dossier

Het leerling dossier is een verzameling van gegevens waar mogelijk verschillende bewaartermijnen voor gelden. Om problemen te voorkomen hanteert Skipov een algemene bewaartermijn die langer is dan de wet veelal voorschrijft, namelijk: 5 kalenderjaren na uitschrijving. Het gaat dan om gegevens zoals:

- Administratieve gegevens, waaronder
  - verzuim/afwezigheid
  - in- en uitschrijving
  - gegevens die nodig zijn om de hoogte van betalingen door de ouder(s) vast te stellen;
- Rapporten van experts zoals psycholoog of logopedist en een behandelplan;
- Doorverwijzingen naar speciaal onderwijs;

De wet geeft niet altijd aan wat de bewaartermijn is. Dit is het geval bij rapporten die te maken hebben met een toets, zoals de entreetoets, citotoets en andere tussentijdse toetsen. Elke basisschool binnen Skipov heeft hierover een eigen beleid. Het gehele leerlingdossier, behalve de NAW-gegevens, wordt 5 kalenderjaren na uitschrijving verwijderd. Skipov maakt namelijk gebruik van de mogelijkheid adresgegevens van leerlingen te bewaren om reünies te organiseren.

Een verzoek van de ouder(s) om een andere bewaartermijn voor gegevens uit het leerling dossier te hanteren kan bij de schooldirecteur worden ingediend. In onderling overleg zal dit naar tevredenheid worden opgelost.

2.4 Het voorkomen van datalekken van leerling gegevens

Naast algemene veiligheidsmaatregelen in de ICT infrastructuur, worden ook specifieke veiligheidsmaatregelen genomen ten aanzien van leerling gegevens.

De verwerking van leerling gegevens heeft met name te maken met het leerling dossier. Zoals al aangegeven wordt binnen Skipov deze informatie alleen vastgelegd en verwerkt als dit noodzakelijk is voor het doel. Dit geldt vooral ten aanzien van gevoelige of bijzondere leerling gegevens.

Het antwoord op de vraag of elk doel van de verwerking van leerling gegevens onder de bescherming van de privacy wetgeving valt is afhankelijk van de praktijk. Het antwoord is ja indien de informatie zowel woord als beeld herleidbaar is tot de individuele leerling. Skipov heeft een aantal veiligheidsmaatregelen genomen om datalekken te voorkomen. Daarbij ligt de focus op het gedrag van de gebruiker. Doel is bewustwording bij de medewerker en de externe partner over het gebruik van hardware, de educatieve en administratief software en de eraan verbonden risico’s op datalekken.

Binnen Skipov wordt gedrag zoveel mogelijk gestuurd door interne richtlijnen. Deze staan gepubliceerd in het Skipov handboek op SharePoint, bijvoorbeeld de Gedragscode Personeel en de de Gedragscode Leerling en Ouder. Alle interne richtlijnen zijn praktisch van aard en doen een beroep op het gezond verstand.

Buiten Skipov wordt gedrag zoveel mogelijk gestuurd door bijvoorbeeld met elke leverancier van (educatieve) software een bewerkersovereenkomst van de PO-raad af te sluiten. Veelal maakt de Digitale bijsluiter Privacy die details geeft over actuele beveiligingsmaatregelen van de leverancier deel uit van deze bewerkersovereenkomst. Ten tijde van de jaarlijkse accountantscontrole wordt de inhoud en reikwijdte van alle bewerkerscontracten objectief gescreend en desgewenst door Skipov als eindverantwoordelijke aangepast.

2.5 Data minimalisatie

Skipov stelt alles in het werk om elke leerling kwalitatief goed onderwijs te garanderen. Hiervoor is verwerking van leerling gegevens nodig. Skipov houdt zich aan de proportionaliteitseis van de privacywetgeving omdat de verwerking van leerling gegevens wordt beperkt tot het doel wat ermee wordt gediend. Daarbij gaat het alleen om die leerling gegevens die nodig zijn de gestelde doelen te bereiken. Deze noodzaak wordt in de privacywetgeving subsidiairiteitseis genoemd. Skipov ziet daarbij het belang om de ouder(s) te informeren en te betrekken.

2.6 Transparantie en Communicatie

Skipov informeert de ouder(s) en de leerling vooraf in begrijpelijke taal over de verwerking van leerling gegevens. De volgende communicatiekanalen worden ingezet om ouder(s) te informeren:

- (Digitale) schoolgids;
- Website van Skipov;
- Via de leerkracht of schooldirecteur.

Onder het kopje Voorkomen Datalekken staan de veiligheidsmaatregelen vermeld om te voorkomen dat tijdens de communicatie inbreuk wordt gemaakt op de privacy van de leerling.

3 Medewerker gegevens in de school

De personeelsgeleding van de GMR heeft instemmingsrecht met betrekking tot de verwerking van persoonsgegevens van de medewerker. Voor dit beleid vallen onder medewerker onder andere: payroll medewerkers, vrijwilligers en sollicitanten. Voor meer details wordt verwezen naar de inleiding.

Als wordt gesproken over de verwerking van persoonsgegevens van de medewerker wordt alles bedoeld wat er onder zou kunnen vallen, zoals het online en offline verzamelen van persoonsgegevens, kopiëren, opslaan, verspreiden, publiceren, delen én het (onderling) uitwisselen. Dit slaat niet alleen op feitelijke informatie, maar ook op foto's, video's en dergelijke. Alles wat hierbij herleidbaar is tot de individuele medewerker valt onder de privacybescherming. Binnen Skipov wordt hierbij geen onderscheid gemaakt tussen geautomatiseerde en handmatige gegevens(verwerking).

In deze paragraaf wordt ingegaan hoe binnen Skipov wordt omgegaan met medewerker gegevens. Met name het doel en de verwerking van medewerker gegevens, het personeelsdossier en de maatregelen die genomen worden ten aanzien van de privacy risico's.

3.1 Doel

De medewerker gaat bij Skipov aan het werk op grond van een schriftelijke afspraak die door de medewerker voor akkoord is ondertekend. Veelal staat in deze afspraak al vermeld of wordt de medewerker mondeling verteld dat Skipov gegevens zal verwerken.

Dat een doel en noodzaak aanwezig is om medewerker gegevens te verwerken is voor een ieder duidelijk. In deze paragraaf ligt het accent dan ook meer op welke gegevens worden verwerkt en hoe de privacy daarbij wordt beschermd. Dit is van belang omdat gegevens van de medewerker vrijwel altijd herleidbaar zijn tot een individuele medewerker.
Het is niet uit te sluiten dat gaandeweg (aanvullende) redenen ontstaan voor het verwerken van medewerker gegevens. In al deze situaties beoordeelt de bestuurder na overleg met het stafkantoor of specifiek toestemming/ akkoord van de medewerker gevraagd zal worden.

Bij dit alles is Skipov zich ervan bewust dat sprake kan zijn van bijzondere of gevoelige persoonsgegevens. Dit zijn persoonsgegevens van de medewerker die extra gevoelige informatie bevatten, zoals bijvoorbeeld gezondheid, (etnische) afkomst, godsdienst of een problematische thuissituatie.
Deze gegevens worden alleen vastgelegd en verwerkt als dit noodzakelijk is voor het doel.

Als de medewerker Skipov verlaat worden de medewerker gegevens niet overgedragen of ter informatie aan derden verstrekt.

3.2 Onze vooraf gestelde doelen met de verwerking van medewerker gegevens

Wetgeving en de CAO die op de medewerker van toepassing is, bepalen de doelen die Skipov kent voor de verwerking van medewerker gegevens.
De doelen zijn onder andere:

- Administratieve verplichtingen door of namens de overheid zoals bijvoorbeeld de belastingdienst;
- Bereikbaarheid en contactgegevens;
- Arbo wetgeving;
- Monitoring van verlof en verzuim;
- Opbouw van pensioen, jubilea en andere rechten;
- Uitbetaling van salaris en reiskosten;
- Gesprekscyclus;
- Professionalisering en loopbaanontwikkeling;

Alle gegevens die te maken hebben met een van bovenstaande doelen en relevant zijn ten aanzien van de individuele medewerker worden verzameld in het personeelsdossier.

3.3 Het personeelsdossier

In het algemeen bestaat het personeelsdossier binnen het onderwijs uit 3 delen:

- Het personeelsdossier.
- Het bekwaamheidsdossier.
- Het verzuimdossier (**niet** te verwarren met het medisch/ ziektedossier).

Het personeelsdossier van medewerkers die op of na 1 januari 2014 bij Skipov werkzaam zijn wordt opgeslagen in HR2Day. Daarnaast wordt van elke medewerker een papieren dossier op de basisschool en/ of het stafkantoor bijgehouden en gearchiveerd in afgesloten dossierkasten.

Het verzuimdossier staat als onderdeel van het personeelsdossier in HR2Day. Dit dossier bevat echter geen medische gegevens. Deze staan in het medisch/ ziekte dossier van de arbodienst.

In de paragraaf ICT staat beschreven hoe in het algemeen de ICT infrastructuur binnen Skipov zodanig is ingericht om de privacy van de medewerker te beschermen en verwerking door onbevoegde personen (onrechtmatige verwerking) uit te sluiten. Dit geldt met name voor administratieve software van een externe partij zoals het al genoemde HR2Day.
Periodiek onderzoekt de systeembeheerder van Skipov of de bescherming nog voldoende is.

Niet alle medewerkers zoals de Payroll medewerker en de vrijwilliger zijn echter in dienst bij Skipov. Daarom is HR2Day zo ingericht dat het personeelsdossier in 2 afzonderlijke digitale omgevingen wordt opgeslagen: Skipov en Skipov extern. Alleen relevante gegevens worden in een personeelsdossier opgenomen. De medewerker kan vragen over het personeelsdossier aan de afdeling Personeelszaken stellen.

Ten aanzien van het personeelsdossier en het verzuimdossier houdt Skipov rekening met de rechten van de medewerker.

3.3.1 Inzagerecht en andere rechten van de medewerker

Ten aanzien van het personeelsdossier heeft in principe de medewerker een:

- Inzagerecht.
  De medewerker kan een afspraak maken met de afdeling Personeelszaken om het dossier in te zien. Alleen informele documenten zoals notities die een persoonlijke mening weergeven en die slechts bedoeld zijn voor intern overleg en/ of documenten die informatie bevatten over collega's mogen van inzage worden uitgesloten.
- Kopierecht.
  Op verzoek van de medewerker verstrekt Skipov een kopie van het personeelsdossier tenzij het dossier te omvangrijk is. In dat geval vraagt Skipov specifiek aan te geven van welke documenten een kopie wordt gewenst. De wachttijd voor de kopie is maximaal 4 kalenderweken.
- Correctierecht met betrekking tot persoonsgegevens.
  Het staat de medewerker vrij om een schriftelijk verzoek bij de schooldirecteur in te dienen om bepaalde gegevens te corrigeren. Dit correctierecht heeft betrekking op het verbeteren, aanvullen, verwijderen, afschermen en weghalen van gegevens als de medewerker vindt dat deze bijvoorbeeld niet relevant zijn en/ of sprake is van onjuistheid of onvolledigheid.
  De afdeling Personeelszaken neemt contact op om een correctieverzoek door te spreken en legt uit wat de uiteindelijke beslissing is.
- Klachtrecht.
  Bij ontevredenheid van de medewerker over de inhoud of het proces van de basisschool of Skipov ten aanzien van het medewerker dossier, vindt eerst een gesprek plaats met de schooldirecteur. Als dit op niets uitdraait, kan de medewerker een beroep doen op de interne klachten procedure van Skipov.

Skipov neemt binnen vier weken een beslissing als een verzoek zoals hierboven vermeld wordt gedaan.

Het correctierecht is beperkt tot strikt feitelijke persoonsgegevens. Persoonsgegevens die niet helemaal feitelijk zijn zoals een voor de medewerker nadelige beoordeling, vallen dus niet onder het correctierecht. Het kan immers niet zo zijn dat een medewerker ''alles wat ongewenst is'' uit het personeelsdossier kan krijgen. Skipov zal in zo'n situatie na goed overleg het standpunt van de medewerker opnemen in het personeelsdossier.

3.3.2 Privacy met betrekking tot het medisch/ ziekte dossier

Skipov houdt zich aan de wetgeving met betrekking tot de zieke medewerker. Met betrekking tot bescherming van de privacy houdt dit in dat medewerker gegevens die te maken hebben met de aard, de oorzaak en het verloop van de ziekte alleen als medisch dossier worden opgeslagen in de onafhankelijke database van de arbodienst. Dit verzuiminformatiesysteem van de arbodienst is alleen toegankelijk voor aldaar geautoriseerde personen zoals de bedrijfsarts. Hierdoor zijn de medische gegevens van de medewerker afgeschermd voor de direct leidinggevende die namens Skipov als casemanager verzuim optreedt.

Alle medische dossiers in de database worden dus door de arbodienst aangemaakt en bijgehouden. Skipov heeft geen inzagerecht of andere rechten. Wel krijgt Skipov van de arbodienst terugkoppeling over de functie gerelateerde situatie zoals de belastbaarheid en de geschiktheid te kunnen werken. Deze informatie wordt, naast de standaard verzuimregistratie-en begeleiding, wel opgeslagen in HR2Day en het papieren dossier.

De medewerker heeft inzagerecht met betrekking tot het medisch dossier.

3.3.3 Inzagerecht door anderen

In bepaalde gevallen is Skipov wettelijk verplicht om informatie over de medewerker aan bepaalde instanties te geven. Die informatie beperkt zich tot wat relevant is. Hierdoor is het niet nodig vooraf toestemming van de medewerker te vragen. Het gaan dan bijvoorbeeld om:

- een verplichting jegens de werknemer na te komen;
- het in overleg inschakelen van een deskundige zoals een vertrouwenspersoon;
- een wettelijke verplichting, bijv. belastingdienst mbt werknemersverzekeringen;
- voor een gerechtvaardigd belang van Skipov op te komen, bijvoorbeeld het verhalen van schade aan eigendommen van Skipov (laptop, mobile telefoon).

3.3.4 Bewaartermijn personeelsdossier

Het personeelsdossier is een verzameling van gegevens waar mogelijk verschillende bewaartermijnen voor gelden. Om problemen te voorkomen hanteert Skipov een algemene bewaartermijn die langer is dan de wet veelal voorschrijft, namelijk: 7 kalenderjaren nadat de medewerker Skipov heeft verlaten.
Het gaat dan om gegevens zoals:

- Salarisadministratie;
- Loonbelastingverklaring;
- Kopie identiteitsbewijs;
- Klachtenprocedure inclusief eventuele inzet van vertrouwenspersoon;

De wet geeft niet altijd aan wat de bewaartermijn is. Dit is het geval bij (gespreks)verslagen van bijvoorbeeld de beoordeling, het functioneren, re-integratiedossier en ontslag. Daarnaast maakt Skipov gebruik van de mogelijkheid adresgegevens van oud medewerkers te bewaren om events zoals bijvoorbeeld reünies te organiseren.

Een verzoek van de medewerker om een andere bewaartermijn voor gegevens uit het personeelsdossier te hanteren kan bij de afdeling Personeelszaken worden ingediend. In onderling overleg zal dit naar tevredenheid worden opgelost.

3.4 Het voorkomen van datalekken van medewerker gegevens

Naast algemene veiligheidsmaatregelen in de ICT infrastructuur, worden ook specifieke veiligheidsmaatregelen genomen ten aanzien van leerling gegevens.

De verwerking van medewerker gegevens heeft met name te maken met het personeelsdossier. Zoals al aangegeven wordt binnen Skipov deze informatie alleen vastgelegd en verwerkt als dit noodzakelijk is voor het doel. Dit geldt vooral ten aanzien van gevoelige of bijzondere medewerker gegevens.

Het antwoord op de vraag of elk doel van de verwerking van medewerker gegevens onder de bescherming van de privacy wetgeving valt is afhankelijk van de praktijk.

Het antwoord is ja indien de informatie zowel woord als beeld herleidbaar is tot de individuele medewerker. Skipov heeft een aantal veiligheidsmaatregelen genomen om datalekken te voorkomen.

Daarbij ligt de focus op het gedrag van de gebruiker. Doel is bewustwording bij het stafkantoor en de externe partner over het gebruik van hardware, de administratieve software en de eraan verbonden risico's op datalekken.

Binnen Skipov wordt gedrag zoveel mogelijk gestuurd door interne richtlijnen. Deze staan gepubliceerd op intranet (SharePoint), zoals bijvoorbeeld Gedragscode Personeel, IPB en de afzonderlijke Handleidingen en instructies die het gebruik van specifieke software en hardware toelichten en randvoorwaarden aangeven. Daarnaast vermeldt het Handboek Skipov nog andere documenten.
Al deze interne richtlijnen zijn praktisch van aard en doen een beroep op het gezond verstand.

Buiten Skipov wordt gedrag zoveel mogelijk gestuurd door bijvoorbeeld met elke leverancier van administratieve software een bewerkersovereenkomst af te sluiten. Veelal maakt de Digitale bijsluiter Privacy die details geeft over actuele beveiligingsmaatregelen van de leverancier deel uit van deze bewerkersovereenkomst. Ten tijde van de jaarlijkse accountantscontrole wordt de inhoud en reikwijdte van alle bewerkerscontracten objectief gescreend en desgewenst door Skipov als eindverantwoordelijke aangepast.

3.5 Data minimalisatie

Skipov stelt alles in het werk om de medewerker te faciliteren en haar verplichtingen als werkgeefster goed na te komen. Hiervoor is verwerking van medewerker gegevens nodig. Skipov houdt zich aan de proportionaliteitseis van de privacywetgeving omdat de verwerking van medewerker gegevens wordt beperkt tot het doel wat ermee wordt gediend. Daarbij gaat het alleen om die medewerker gegevens die nodig zijn de gestelde doelen te bereiken.
Deze noodzaak wordt in de privacywetgeving subsidiairiteitseis genoemd.

3.5.1 Transparantie en Communicatie

Skipov informeert de medewerker vooraf in begrijpelijke taal over de verwerking van gegevens. De volgende communicatiekanalen worden ingezet:

- Intranet (SharePoint);
- Verslagen en brieven;
- Website (van zowel school als Skipov);
- School account.