Informatiebeveiligings- en privacybeleid (IBP)

Versie: 20230119

skopos

Inhoudsopgave

Inleiding

Leerlingen hebben recht op een veilige leeromgeving en medewerkers op een veilige werkomgeving. Daar hoort ook bij dat hun privacy goed wordt beschermd. Privacy is niet zomaar iets: het is een grondrecht. Net als het recht op vrijheid van godsdienst of het recht op vrijheid van meningsuiting. In de Universele Verklaring van de Rechten van de Mens is privacy geborgd als mensenrecht. In Europa is privacy vastgelegd in artikel 8 van het Europees Verdrag voor de Rechten van de Mens. En sinds 1983 is privacybescherming opgenomen in artikel 10 van de Nederlandse Grondwet. Artikel 8 van het Europees Handvest voor de Rechten van de Mens ziet specifiek op de bescherming van persoonsgegevens en luidt:

Artikel 8 Bescherming van persoonsgegevens
1. Eenieder heeft recht op bescherming van de hem betreffende persoonsgegevens.
*2. Deze gegevens moeten **eerlijk** worden verwerkt, voor **bepaalde doeleinden** en met toestemming van de betrokkene of op basis van een andere **gerechtvaardigde grondslag** waarin de wet voorziet. Eenieder heeft **recht op toegang** tot de over hem verzamelde gegevens en op **rectificatie** daarvan.*
3. Een onafhankelijke autoriteit ziet toe op de naleving van deze regels.

Vanaf 25 mei 2018 geldt voor alle landen van de EU de Algemene Verordening Gegevensbescherming (AVG). Daarin zijn basisbeginselen opgenomen waar iedere verwerking van persoonsgegevens aan moet voldoen. In Nederland geldt daarnaast de Uitvoeringswet op de AVG (UAVG) en diverse wetgeving waarin regels zijn opgenomen voor specifieke verwerkingen van persoonsgegevens. Relevante wetgeving is onder meer:

- Wet op het primair onderwijs
- Wet op het onderwijstoezicht
- Wet medezeggenschap op scholen
- Archiefwet
- Leerplichtwet
- Auteurswet
- Wetboek van Strafrecht

Om de privacy van de leerlingen en medewerkers te beschermen en een zorgvuldige verwerking van hun persoonsgegevens te waarborgen is een beleid over de omgang met persoonsgegevens noodzakelijk. In de AVG wordt dit het gegevensbeschermingsbeleid genoemd (art. 24 AVG). Dit Informatiebeveiligings- en privacy beleid (IBP-beleid) is de vastlegging van dat beleid.

Dit IBP-beleid is erop gericht om de kwaliteit van de verwerking van informatie en de beveiliging van persoonsgegevens te optimaliseren waarbij er een juiste balans moet zijn tussen privacy, functionaliteit en veiligheid. Het uitgangspunt is dat de persoonlijke levenssfeer van de betrokkenen (zoals leerlingen, medewerkers, ouders/verzorgers) wordt gerespecteerd en Stichting SKOPOS voldoet aan de relevante wet- en regelgeving.

Dit IBP-beleid, wat is opgesteld door het privacyteam van Stichting SKOPOS, is ter instemming voorgelegd aan de GMR en ter goedkeuring aan het bestuur.

Versiebeheer

Datum	Auteur	Versie	Status	Aanpassing
20230119	Carly van den Akker	1	ter goedkeuring	-

Goedgekeurd

Datum	Naam goedkeurder	Status	Handtekening

Leeswijzer IBP Beleid en bijlagen

De opbouw van het IBP-beleid is zo gekozen dat in de tekst van dit document de algemene uitgangspunten zijn opgenomen. Deze zijn gebaseerd op de geldende privacyregelgeving en geven weer op welke wijze deze binnen Stichting SKOPOS wordt geïmplementeerd. Daarnaast zijn de specifieke uitvoeringsdocumenten met de nadere concrete of praktische invulling van de uitvoering van de privacyregelgeving opgenomen in de bijlagen bij dit IBP-beleid, dan wel wordt verwezen naar de vindplaats van deze documenten. Voor deze opzet is gekozen, omdat de bijlagen en de documenten waarnaar wordt verwezen regelmatig kunnen wijzigen als wijzigingen in de verwerking van de persoonsgegevens optreden. Om te voorkomen dat voor iedere wijziging in die uitvoeringsdocumenten het IBP-beleid opnieuw zou moeten worden vastgesteld zijn deze opgenomen in afzonderlijke documenten. Indien een bijlage wijzigt zal dat via de ‘nieuwsbrief ICT & Privacy’ worden aangegeven.

Hoofdstuk 1: Doel van informatiebeveiliging en privacy

1.1. Waarom is informatiebeveiliging en privacy belangrijk?

Het onderwijs is in toenemende mate afhankelijk van informatie en ICT. De hoeveelheid informatie, waaronder persoonsgegevens, neemt toe door o.a. ontwikkelingen als gepersonaliseerd leren met ICT. Het is belangrijk om informatie goed te beschermen en veilig en verantwoord met persoonsgegevens om te gaan. De afhankelijkheid van ICT en persoonsgegevens brengt nieuwe kwetsbaarheden en risico's met zich mee. Het goed regelen van informatiebeveiliging en privacy in een IBP-beleid is noodzakelijk om de gevolgen van deze risico's tot een aanvaardbaar niveau te reduceren en de voortgang van het onderwijs en de bedrijfsvoering optimaal te kunnen waarborgen.

1.2. Toelichting informatiebeveiliging

Onder informatiebeveiliging wordt verstaan het nemen en onderhouden van een hoeveelheid samenhangende maatregelen zodat de betrouwbaarheid van de informatievoorziening gegarandeerd kan worden.

Informatiebeveiliging richt zich op de volgende aspecten (zie ook hoofdstuk 4, paragraaf 1):

- *Beschikbaarheid*: de mate waarin gegevens en/of functionaliteiten beschikbaar zijn op de juiste momenten;
- *Integriteit*: de mate waarin gegevens en/of functionaliteiten juist en volledig zijn;
- *Vertrouwelijkheid*: de mate waarin de toegang tot gegevens en/of functionaliteiten beperkt is tot degenen die daartoe bevoegd zijn.

Onvoldoende informatiebeveiliging kan leiden tot ongewenste risico's in het onderwijsproces en bij de bedrijfsvoering van de instelling. Incidenten en inbreuken in deze processen kunnen leiden tot financiële schades en imagoverlies.

Het treffen van fysieke, procedurele, organisatorische en technische maatregelen is daarvoor van belang, maar de naleving is essentieel. Dit raakt zowel de professionaliteit van de individuele medewerker als de professionele cultuur als geheel. Om een beheersbare en betrouwbare informatievoorziening te behouden, is het van belang dat iedereen een aantal gemeenschappelijke uitgangspunten hanteert en deze uitdraagt. Er dient daarom constante aandacht te zijn voor het verhogen van het beveiligingsbewustzijn van al onze medewerkers en onze partners.

1.3. Toelichting privacy

Privacy ziet toe op de persoonlijke levenssfeer van ieder individu. Daarbij horen ook persoonsgegevens. De AVG regelt onder welke voorwaarden persoonsgegevens verwerkt mogen worden. Persoonsgegevens mogen alleen verwerkt worden als dat gebaseerd is op een wettelijke grondslag, een gerechtvaardigd doel is vastgesteld, ervoor wordt gezorgd dat de gegevens juist zijn, deze niet langer worden bewaard dan nodig en passend worden beschermd. Daarbij geldt als uitgangspunt dat niet meer persoonsgegevens mogen worden verwerkt dan noodzakelijk om de vastgestelde doelen te bereiken ('dataminimalisatie'). Bovendien heeft ieder individu het recht om te weten wat er met zijn persoonsgegevens gebeurt en deze in te zien.

De AVG kent een verantwoordingsplicht. Dat betekent dat de verwerkingsverantwoordelijke moet kunnen aantonen dat wordt voldaan aan de beginselen van de verwerking van persoonsgegevens. De verwerkingsverantwoordelijke is de entiteit die het doel en de middelen voor de verwerking van persoonsgegevens vaststelt. In het kader van dit IBP-beleid is Stichting SKOPOS, de verwerkingsverantwoordelijke voor de verwerking van de persoonsgegevens van alle leerlingen en medewerkers.

Vervlechting informatiebeveiliging en privacy

Informatiebeveiliging is een belangrijke voorwaarde voor de bescherming van ieders privacy, terwijl omgekeerd de zorgvuldige omgang met persoonsgegevens noodzakelijk is voor informatiebeveiliging. Informatiebeveiliging en privacy staan naast elkaar en zijn van elkaar afhankelijk, en worden daarom samengevoegd tot één proces: IBP. Dit IBP-beleid vormt daarom de basis voor informatiebeveiliging en privacy binnen Stichting SKOPOS en vormt de kapstok voor alle afspraken en procedures over de omgang met en de bescherming van persoonsgegevens.

Hoofdstuk 2: Wat is de reikwijdte van dit IBP-beleid?

Relevante begrippen
Om een goede omgang met persoonsgegevens te kunnen waarborgen is het allereerst van belang dat er duidelijkheid bestaat over de relevante begrippen. De privacyregelgeving geldt voor iedere verwerking van persoonsgegevens. De begrippen persoonsgegeven en verwerking worden zeer ruim uitgelegd door de toezichthouders, waaronder de Autoriteit Persoonsgegevens.

Een *persoonsgegeven* is ieder gegeven dat herleidbaar is tot een natuurlijk persoon (de betrokkene), zoals een leerling, een medewerker of een ouder. Persoonsgegevens zijn bijvoorbeeld contactgegevens op een leerlingenlijst, alle gegevens in het LAS, rapporten, zorgplannen, een kopie van een paspoort van medewerkers en salarisgegevens.

Verwerking van persoonsgegevens is iedere handeling die betrekking heeft op persoonsgegevens. Het hoeft geen actieve handeling te zijn. Het kunnen inzien, bewaren, verstrekken of uitsluitend opslaan of vernietigen van persoonsgegevens valt allemaal onder het begrip verwerken.

Bijzondere persoonsgegevens zijn extra gevoelige persoonsgegevens die in principe niet verwerkt mogen worden. Het gaat onder meer om gegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen of het lidmaatschap van een vakbond
blijken, genetische (DNA/RNA) of biometrische gegevens met het oog op de unieke identificatie van een persoon, gegevens over gezondheid, iemands seksueel gedrag of strafrechtelijke gegevens.

2.1. Op wie heeft dit IBP-beleid betrekking?

Het IBP-beleid heeft betrekking op het verwerken van persoonsgegevens van alle betrokkenen binnen Stichting SKOPOS, waaronder in ieder geval alle medewerkers, leerlingen, ouders of verzorgers, (geregistreerde) bezoekers en externe relaties (inhuur/outsourcing), evenals op overige betrokkenen waarvan Stichting SKOPOS persoonsgegevens verwerkt.

2.2. Verwerkingsregisters

Het is niet mogelijk om te weten of wordt voldaan aan de privacyregelgeving, laat staan dat het mogelijk is om aan te tonen dat aan de AVG wordt voldaan als niet bekend is welke verwerkingen van persoonsgegevens plaatsvinden binnen Stichting SKOPOS. Op grond van artikel 30, lid 1 AVG is het verplicht om een verwerkingsregister bij te houden waarin de verwerkingen zijn opgenomen. Iedere verwerkingsverantwoordelijke zal in een verwerkingsregister moeten bijhouden welke categorieën van persoonsgegevens voor welke doelen worden verwerkt, wie de interne en externe ontvangers zijn van die gegevens, of gegevens buiten de EU worden verwerkt, welke bewaarcriteria gelden en welke beveiligingsmaatregelen zijn getroffen. Zie **bijlage 11**. Een deel van de verwerkingen vindt plaats op stichtingsniveau. Daarnaast worden persoonsgegevens verwerkt binnen de scholen van Stichting SKOPOS. Om een zo compleet mogelijk beeld te hebben en te voldoen aan de registerplicht van de AVG is het verwerkingsregisters gevuld met betrekking tot de diverse categorieën van betrokkenen. Stichting SKOPOS zal onder begeleiding van de Functionaris van de Gegevensbescherming een verwerkingsregister vullen en onderhouden.

2.2.1. Leerlingen

De eerste categorie van betrokkenen zijn alle leerlingen van de scholen die vallen onder Stichting SKOPOS. Op stichtingsniveau vinden verwerkingen plaats van leerlinggegevens. Daarnaast vinden de meeste verwerkingen van leerlinggegevens plaats binnen de scholen. Deze registers van verwerkingsactiviteiten van de verwerkingen die betrekking hebben op persoonsgegevens van leerlingen worden bewaard op stichtingsniveau.

2.2.2. Medewerkers

De tweede categorie van betrokkenen zijn alle medewerkers in loondienst bij Stichting SKOPOS. Op stichtingsniveau vinden de meeste verwerkingen plaats van deze gegevens, zoals de personeelsadministratie, de salarisadministratie en opleidingen. Bij de scholen worden persoonsgegevens van medewerkers met name voor praktische werkzaamheden verwerkt, zoals in het kader van de formatie, roosters en het taakbeleid. De registers van verwerkingsactiviteiten met betrekking tot medewerkers worden bewaard op stichtingsniveau.

2.2.3. Ouders en/of verzorgers

Niet alleen van de leerlingen, maar ook van hun ouders en/of verzorgers worden persoonsgegevens verwerkt op stichtingsniveau en met name binnen de scholen. Deze verwerkingen zijn opgenomen in het register van de leerlingen.

2.2.4. Overige betrokkenen

Naast verwerkingen van leerlingen, medewerkers en ouders/verzorgers worden zowel binnen de stichting als op de scholen persoonsgegevens verwerkt van andere personen, zoals invalkrachten, uitzendkrachten, leveranciers van diverse (leer)middelen en externe zorgverleners. Deze verwerkingen zijn opgenomen op die plaatsen waar deze relevant zijn in het verwerkingsregister van leerlingen, dan wel die van medewerkers.

2.3. Begrenzing van de verwerking van persoonsgegevens

De ingevulde registers van verwerkingsactiviteiten vormen de begrenzing van de verwerking van persoonsgegevens binnen Stichting SKOPOS. Op grond van de AVG dienen de doelen voor de verwerking van persoonsgegevens uitdrukkelijk te zijn omschreven en mogen niet meer gegevens worden verwerkt dan noodzakelijk is om die doelen te bereiken. De doelen en categorieën van persoonsgegevens staan omschreven in de verwerkingsregisters. Dat betekent dat Stichting SKOPOS en de onder haar verantwoordelijkheid vallende personen geen persoonsgegevens mogen verwerken die niet in de verwerkingsregisters zijn opgenomen. Tevens mogen de persoonsgegevens die beschikbaar zijn niet voor andere doelen worden verwerkt die niet verenigbaar zijn met de doelen die in de registers zijn opgenomen. Stichting SKOPOS zal zorgdragen voor bewustwording bij alle personen die de persoonsgegevens verwerken en onder haar verantwoordelijkheid vallen. Daarbij zal Stichting SKOPOS in samenspraak met de directeuren van de scholen zorgen dat de leerkrachten, administratieve ondersteuners en andere betrokken personen werkinstructies krijgen in dat kader. Ook zal Stichting SKOPOS in de persoon van de FG erop toezien dat de feitelijke verwerkingen beperkt blijven door dat steekproefsgewijs te controleren. Met deze maatregelen wordt door Stichting SKOPOS geborgd dat niet meer persoonsgegevens worden verwerkt dan noodzakelijk is voor de vastgestelde doelen.

Hoofdstuk 3: Rol en taken van Stichting SKOPOS

3.1. Rol als verwerkingsverantwoordelijke

Als Verwerkingsverantwoordelijke zal het bestuur moeten voldoen aan de AVG en andere relevante wet- en regelgeving inzake de verwerking van persoonsgegevens. Stichting SKOPOS neemt de verantwoordelijkheid om ervoor te zorgen dat de benodigde documenten worden opgesteld, de vereiste afspraken worden gemaakt met externe partijen en de personen die onder zijn verantwoordelijkheid persoonsgegevens verwerken voldoende instructies en informatie verkrijgen om een passende bescherming van de persoonsgegevens te waarborgen. Het bestuur is hierop aan te spreken en legt hier verantwoording over af. Een goede balans tussen het belang van het bestuur om persoonsgegevens te verwerken en het belang van de betrokkenen voor de bescherming van zijn/haar persoonsgegevens wordt vooropgesteld. In het privacyreglement in **bijlage 1** heeft Stichting SKOPOS de verdere uitwerking voor de omgang met en verwerking van persoonsgegevens op een rij gezet.

3.2. Taken en verantwoordelijkheden

Stichting SKOPOS heeft de taak en de verantwoordelijkheid om een zorgvuldige omgang met persoonsgegevens en de naleving van de AVG en andere relevante regelgeving te waarborgen.
In dat kader is vanuit Stichting SKOPOS een privacy-regiegroep aangesteld om de verdere implementatie van de AVG en aanverwante privacyregelgeving te coördineren. Daarnaast maakt Stichting SKOPOS gebruik van een externe FG.
Stichting SKOPOS heeft een privacyteam dat zorg draagt voor het uitvoeren van
het privacybeleid op de individuele scholen. Het privacyteam bestaat uit meerdere personen, waaronder een privacycoördinator die periodiek overleg heeft met de externe FG.
Daarnaast neemt Stichting SKOPOS deel aan de AVG-denktank met Stichting Talentis en Stichting Cadans Primair.

3.2.1 Voorlichting en bewustwording binnen de organisatie

Beleid en maatregelen zijn niet voldoende om persoonsgegevens passend te beschermen. De feitelijke omgang met persoonsgegevens door alle personen die werkzaam zijn voor of onder de verantwoordelijkheid vallen van Stichting SKOPOS dient zorgvuldig te zijn en in overeenstemming met de AVG. Dat

betekent dat al deze personen de persoonsgegevens die zij verwerken, geheim dienen te houden. Dit wordt geregeld d.m.v. een geheimhoudingsverklaring. Zie **bijlage 9**.
Om dit te bevorderen zorgt Stichting SKOPOS met hulp van het privacyteam voor diverse bewustwordingscampagnes voor medewerkers. Zowel via nieuwsbrieven als in workshops (per groep gebruikers), wordt aandacht gegeven aan de relevantie van een zorgvuldige omgang met persoonsgegevens en wat zorgvuldige omgang inhoudt. Ook ouders worden geïnformeerd via nieuwsbrieven. Daarmee wordt het bewustzijn van de medewerkers voortdurend aangescherpt, zodat de kennis van risico's wordt verhoogd en veilige en verantwoorde omgang met persoonsgegevens wordt aangemoedigd.

Verhoging van het IBP-bewustzijn binnen Stichting SKOPOS is een gezamenlijke verantwoordelijkheid van het privacyteam en bestuur.

3.2.2. Handreiking AVG

Binnen Stichting SKOPOS is het veilig en betrouwbaar omgaan met informatie de verantwoordelijkheid van iedereen. Hierbij hoort niet alleen het actief bijdragen aan de veiligheid van geautomatiseerde systemen en de daarin opgeslagen informatie, zoals met sterke wachtwoorden of wachtzinnen, maar ook de bescherming van papieren documenten. Daarnaast zijn er afspraken over het gebruik van internet en sociale media. Zie **bijlage 4**. Stichting SKOPOS heeft een handreiking die specifiek toeziet op een veilige omgang met persoonsgegevens. Deze handreiking is opgenomen na **bijlage 5** en wordt na een gezamenlijke workshop digitaal verspreid onder alle medewerkers.

3.2.3. Verdeling van verantwoordelijkheden

Het bestuur is op grond van haar rol als verwerkingsverantwoordelijke eindverantwoordelijk voor de naleving van de privacyregelgeving. Stichting SKOPOS heeft echter geen direct zicht op de verwerkingen die zich afspelen bij de individuele scholen. Naast het hiervoor genoemde privacyteam, de privacycoördinator en externe FG hebben meerdere personen een concrete rol met daarbij horende taken met betrekking tot de naleving van deze regelgeving. Een schema van deze rollen en verantwoordelijkheden is opgenomen in **bijlage 2**.

3.2.4. Functionaris voor de Gegevensbescherming (FG)

De FG levert een bijdrage aan het ontwikkelen, bewaken en evalueren van de procedures, planningen en instrumenten in het kader van de AVG. De FG houdt tevens toezicht op de naleving van de AVG. De FG verricht zijn werkzaamheden voor Stichting SKOPOS en rapporteert jaarlijks aan het bestuur, aan de directeuren en aan de GMR. De functiebeschrijving van de FG bevindt zich in **bijlage 3**.

Hoofdstuk 4: Informatiebeveiliging en meldplicht datalekken

4.1. Classificatie en risicoanalyse

De AVG schrijft voor dat de verwerkingsverantwoordelijke passende technische en organisatorische maatregelen dient te treffen om een op het risico afgestemd beveiligingsniveau te waarborgen. Bij de beoordeling van het passende beveiligingsniveau dient met name rekening te worden gehouden met de verwerkingsrisico's, vooral als gevolg van de vernietiging, het verlies, de wijziging of de ongeoorloofde toegang tot persoonsgegevens (artikel 32 AVG). Alle gegevens en informatiesystemen waarop dit IBP-beleid van toepassing is, wordt geclassificeerd om te bepalen welke beveiligingsmaatregelen passend zijn. Het niveau van de te nemen beveiligingsmaatregelen is namelijk afhankelijk van de classificatie. De classificatie van informatie is afhankelijk van de gegevens in het concrete informatiesysteem en wordt bepaald op basis van risicoanalyses. Daarbij zijn beschikbaarheid, integriteit en vertrouwelijkheid de betrouwbaarheidsaspecten die van belang zijn. De classificatie is opgenomen in het verwerkingsregister.

4.1.1. Plan-do-check-act cyclus

Om de beveiliging van persoonsgegevens passend te houden zal op gezette tijden getest, beoordeeld en geëvalueerd moeten worden of de getroffen maatregelen doeltreffend zijn of dat aanpassing vereist is. De maatregelen die getroffen zijn, zijn opgenomen in de rapportages van de FG. Deze worden bewaard op bestuursniveau.
Bij wijzigingen in de infrastructuur of de aanschaf van nieuwe (informatie)systemen zal vóóraf gekeken moeten worden naar de impact van de ontwikkelingen en de beoogde verwerkingen op informatiebeveiliging, zodat passende maatregelen genomen kunnen worden. Zo zal vanaf de start van nieuwe (ICT)projecten rekening moeten worden gehouden met informatiebeveiliging.

Om de privacy risico's van een gegevensverwerking in kaart te brengen, kan een data protection impact assessment (DPIA) worden uitgevoerd. Hierna kunnen maatregelen worden getroffen om deze risico's te verkleinen.

4.1.2. Logging en monitoring

Geautomatiseerde systemen worden automatisch gelogd en gemonitord en toegang tot gegevens wordt vastgelegd. Hieronder vallen onder andere het in- en uitloggen van gebruikers en (pogingen) tot ongeautoriseerde toegang tot het netwerk.

4.2. Meldplicht beveiligingsincidenten en datalekken

Een beveiligingsincident is een gebeurtenis waarbij de mogelijkheid bestaat dat de beveiliging van informatie of informatie verwerkende systemen in gevaar is of kan komen.
Een datalek is een beveiligingsincident; waarbij persoonsgegevens verloren raken of onrechtmatig worden verwerkt, zoals het sturen van een e-mail met leerlingenlijst naar de verkeerde ontvanger of het verlies van een USB-stick met een personeelsdossier. Een datalek dient gemeld te worden aan de Autoriteit Persoonsgegevens, tenzij het datalek geen risico's inhoudt voor de betrokkene(n). Tevens dient de verwerkingsverantwoordelijke de betrokkene(n) te informeren indien het datalek een groot risico inhoudt voor de betrokkene(n). Bijvoorbeeld bij het lekken van inloggegevens of gegevens die gebruikt kunnen worden om identiteitsfraude te plegen (BSN of kopie ID-bewijs).

4.2.1. Procedure beveiligingsincidenten en meldplicht datalekken

Alle medewerkers, die een beveiligingsincident of datalek vermoeden dienen dit te melden bij het privacyteam van Stichting SKOPOS. Het melden van datalekken is vastgelegd in een protocol dat is opgenomen in **bijlage 6**. Voor afhandeling van deze incidenten volgt een gestructureerd proces, dat ook voorziet in de juiste stappen rondom de meldplicht datalekken. Alle (beveiligings)incidenten worden vastgelegd in een incidentenregister. Periodiek zullen de datalekken besproken worden met de FG en directeur-bestuurder.

Hoofdstuk 5: Afspraken met derden

5.1. Overzicht van derden en de rol van deze derden

De AVG en ook de overige privacyregelgeving maakt een onderscheid tussen twee rollen, namelijk de verwerkingsverantwoordelijke en de verwerker. Zoals in hoofdstuk 3 toegelicht geldt het bestuur als verwerkingsverantwoordelijke in de zin van de AVG en zal zij moeten voldoen aan haar verantwoordingplicht.

De verwerker is degene die persoonsgegevens verwerkt ten behoeve van een verwerkingsverantwoordelijke. Een verwerker heeft geen eigen doel voor de verwerking van de persoonsgegevens buiten het uitvoeren van de dienstverlening voor het bestuur. Een verwerker heeft op grond van de privacywetgeving veel minder verplichtingen. Een verwerker dient de
persoonsgegevens geheim te houden, mag deze niet voor een ander doel verwerken dan in het kader van de opdracht van de verwerkingsverantwoordelijke en zal moeten zorgdragen voor een passende beveiliging van de persoonsgegevens. Een verwerker heeft echter onder meer geen eigen grondslag of doel voor de verwerking nodig, heeft geen informatieplicht richting betrokkenen, hoeft geen datalekken te melden bij de Autoriteit Persoonsgegevens en hoeft niet rechtstreeks te reageren op verzoeken van betrokkenen. Het bestuur is verantwoordelijk voor de juiste omgang met de persoonsgegevens, ook als bepaalde verwerkingen worden uitbesteed aan een verwerker. Door middel van afspraken hierover in de overeengekomen verwerkersovereenkomsten met de verwerkers (veelal leveranciers) wordt dit beoogd. In deze overeenkomsten worden afspraken gemaakt ter bescherming van de persoonsgegevens. Zo zorgt Stichting SKOPOS ervoor dat derde partijen voor doelen en onder voorwaarden die Stichting SKOPOS met hen heeft afgesproken, persoonsgegevens verwerkt.

De verwerkers waar Stichting SKOPOS gebruik van maakt voor haar scholen zijn onder meer de leveranciers van digitale leermiddelen, het leerling-administratiesysteem, de leerlingvolgsystemen en de beheerder van de digitale infrastructuur binnen alle scholen. Daarnaast maakt Stichting SKOPOS gebruik van partijen die de personeelsadministratie onderhouden en beheren en partijen die worden ingeschakeld in het kader van de werving- en selectie van nieuwe medewerkers voor Stichting SKOPOS. De partijen waarmee Stichting SKOPOS gegevens uitwisselen worden opgenomen in de betreffende verwerkingsregisters.

5.1.1. *Afspraken met verwerkers*

Indien het bestuur verwerkers inschakelt, zal zij een verwerkersovereenkomst moeten sluiten met deze partijen. De PO-Raad, de VO-raad, MBO-raad en leden van brancheorganisaties en verschillende leveranciers van digitale onderwijsmiddelen en informatiesystemen hebben het Convenant Digitale Onderwijsmiddelen en Privacy afgesloten. Dit convenant is in overeenstemming met de vereisten van de AVG opgesteld en bevat als bijlage een Model Verwerkersovereenkomst. Indien het bestuur gebruik maakt van de diensten van verwerkers volgt zij de richtlijnen en adviezen van de PO-raad en sluit met deze partijen de verwerkersovereenkomst conform genoemd model. De gesloten verwerkersovereenkomsten worden door de privacycoördinator bijgehouden in het verwerkingsregister en worden bewaard op bestuursniveau.

5.1.2. *Afspraken met andere partijen*

Het kan ook voorkomen dat de derde waarmee persoonsgegevens worden uitgewisseld of die persoonsgegevens verwerkt voor Stichting SKOPOS, een bepaalde zeggenschap heeft over de verwerking van deze gegevens. Zoals een zorgverlener die een leerling begeleidt of de bedrijfsarts die een zieke medewerker op spreekuur krijgt. In dat geval is die derde ook een verwerkingsverantwoordelijke en geen verwerker. Het convenant of de verwerkersovereenkomst zijn dan niet van toepassing.

Indien de andere partij gezamenlijk met het bestuur het doel voor de gegevensverwerking bepaalt zijn partijen gezamenlijke verwerkingsverantwoordelijken en zullen zij op grond van artikel 26 AVG een regeling moeten vastleggen over de omgang met persoonsgegevens. Als de andere partij andere doelen heeft voor de verwerking van persoonsgegevens dan het bestuur, gelden beide partijen als afzonderlijke verwerkingsverantwoordelijken. Er is geen wettelijke verplichting opgenomen in de AVG voor het sluiten van een overeenkomst tussen twee afzonderlijke verwerkingsverantwoordelijken.

Voor de gegevensuitwisseling met andere partijen kan worden gewerkt met een online registratiesysteem (zoals Parnassys of Esis). Er is dan beperkte autorisatie mogelijk. Ouders (met gezag) hebben naast de informatieplicht o.g.v. de onderwijswetgeving (tot 18 jaar) ook het recht o.g.v. de AVG verzoeken over de persoonsgegeven van hun kinderen tot 16 jaar (net als andere mogelijke betrokkenen) in te dienen, ze hebben net als de andere betrokkenen de volgende rechten:

- Het recht op inzage;
- Het recht op informatie;
- Het recht op rectificatie;
- Het recht op vergetelheid en gegevenswissing;
- Het recht op dataportabiliteit;
- Het recht op beperking van de verwerking;
- Het recht op een menselijk blik bij besluitvorming;
- Het recht van bezwaar;
- Het recht om een klacht in te dienen bij de Functionaris Gegevensbescherming of de Autoriteit Persoonsgegevens.

Er is een protocol Rechten van betrokkenen binnen Stichting SKOPOS.

Het bestuur zal ten aanzien van de door haar ingeschakelde derden samen met het privacyteam bepalen welke rol die hebben, óf en welke afspraken gemaakt moeten worden en houdt dit bij in het verwerkingsregister.

5.2. Verdeling taken voor het maken van afspraken tussen bestuur en de school

De privacycoördinator maakt een overzicht van de partijen waarmee verwerkersovereenkomsten gesloten moeten worden. Dat geldt in ieder geval voor die partijen die diensten aan het bestuur of aan een of meerdere scholen verlenen. Daarnaast zal het voorkomen dat scholen specifieke diensten uitbesteden aan derde partijen. Bijvoorbeeld in het kader van specifieke activiteiten die door de school worden aangeboden, zoals een fotograaf of leverancier van oudertevredenheidsonderzoeken. Ook die verwerkersovereenkomsten worden door de privacycoördinator gecontroleerd en ter ondertekening aangeboden aan de directeur-bestuurder.

Hoofdstuk 6: Transparantie en rechten betrokkenen

6.1. Verantwoordingsplicht

De invulling van de verantwoordingsplicht onder de AVG wordt aangetoond door:

Beleid. Het hebben van een geïmplementeerd informatiebeveiligings- en privacybeleid. Het informatiebeveiligingsbeleid van Stichting SKOPOS is verbonden met dit privacybeleid. In het informatiebeveiligingsbeleid staan een aantal passages die betrekking hebben op de beveiliging van persoonsgegevens zoals welke principes gehanteerd worden ten aanzien van te verlenen autorisaties.

Verwerkingsregister. Stichting SKOPOS moet een register bijhouden van alle verwerkingsactiviteiten die door of namens Stichting SKOPOS plaatsvinden. In dit register moeten onder meer worden opgenomen: de categorieën van betrokkenen, de soorten persoonsgegevens en met wie deze gegevens gedeeld worden. Voor betrokkenen moet duidelijk zijn welke persoonsgegevens worden vastgelegd, verwerkt, waarom en door wie. Per verwerking wordt aangegeven wie de verwerkingsverantwoordelijke is, wie beheerder is en (indien van toepassing) wie verwerker is.

Gegevensbeschermingseffectbeoordeling (GEB) of Data Protection Impact Assessment (DPIA). Wanneer een verwerking van persoonsgegevens waarschijnlijk veel risico's inhoudt voor betrokkenen, moet Stichting SKOPOS vooraf beoordelen wat het effect hiervan is op de bescherming van persoonsgegevens. Er moet dus van tevoren worden gekeken wat de risico's zijn en of die ondervangen kunnen worden.

Procedure datalekken. Er is sprake van een datalek wanneer persoonsgegevens zijn vernietigd of verloren, gewijzigd, verstrekt of toegankelijk gemaakt op een manier die in strijd is met de AVG. Wanneer er sprake is van een datalek, moet Stichting SKOPOS, als verwerkingsverantwoordelijke, dit zo spoedig mogelijk melden bij de toezichthouder (de Autoriteit Persoonsgegevens) zo mogelijk binnen 72 uur. Wanneer er grote kans bestaat dat het datalek negatieve gevolgen heeft voor betrokkenen, moeten deze ook worden gewaarschuwd.

6.2. Informeren ouders, leerlingen en medewerkers

Iedere betrokkene heeft het recht om te weten welke persoonsgegevens van hem worden verwerkt, voor welke doeleinden, wie de ontvangers zijn, wat hun rechten zijn, etc. Dit brengt mee dat Stichting SKOPOS de verplichting heeft om de betrokkenen daarover te informeren. De ouders moeten helder en begrijpelijk worden geïnformeerd over de omgang met de persoonsgegevens van hun kinderen en van henzelf. Stichting SKOPOS heeft daarvoor een privacyverklaring op de website geplaatst ("Stichting SKOPOS en de Algemene Verordening Gegevensbescherming (AVG)") en op alle websites van de scholen zal op de homepage dezelfde privacyverklaring moeten staan. De ouders en/of verzorgers van de leerlingen zullen op die verklaring worden gewezen d.m.v. de schoolgids.

Ook de medewerkers moeten helder en begrijpelijk worden geïnformeerd over de omgang met hun persoonsgegevens. Zie de privacyverklaring voor medewerkers, **bijlage 1**.

6.3. Werkwijze voor rechten betrokkenen

De AVG geeft betrokkenen verschillende rechten t.a.v. haar of zijn gegevens wanneer deze verwerkt worden door organisaties. Dit zijn:

- Het recht op inzage;
- Het recht op informatie;
- Het recht op rectificatie;
- Het recht op vergetelheid en gegevenswissing;
- Het recht op dataportabiliteit;
- Het recht op beperking van de verwerking;
- Het recht op een menselijk blik bij besluitvorming;
- Het recht van bezwaar;
- Het recht om een klacht in te dienen bij de Functionaris Gegevensbescherming of de Autoriteit Persoonsgegevens.

Betrokkenen kunnen op meerdere manieren een verzoek indienen: digitaal, schriftelijk of mondeling. Organisaties zijn verplicht om binnen één maand te reageren op dit verzoek.

In de privacyverklaring worden de betrokkenen gewezen op deze rechten. De rechten van betrokkenen worden vertaald in heldere, laagdrempelige procedures en worden helder gecommuniceerd richting de betrokkenen.
Daarbij geldt als uitgangspunt dat bij een dergelijk verzoek de medewerker die het verzoek binnenkrijgt deze doorgeeft aan de directeur van de school waar de medewerker werkzaam is. De directeur zal het verzoek in samenspraak met het privacyteam behandelen. Indien de medewerker op het bestuurskantoor werkzaam is, zal deze het verzoek doorsturen aan de privacycoördinator.

Stichting SKOPOS informeert de betrokkene(n) actief over de verwerking van hun persoonsgegevens, is transparant over het verwerken van de persoonsgegevens en verstrekt deze informatie, conform artikel 12 AVG, in een begrijpelijke vorm. Hierin wordt in ieder geval de volgende informatie vermeld:
de contactgegevens van Stichting SKOPOS;
de contactgegevens van de Functionaris voor Gegevensbescherming van Stichting SKOPOS;
de doeleinden van de gegevensverwerking en de grondslagen voor de verwerking;
een omschrijving van de belangen van Stichting SKOPOS indien de verwerking wordt gebaseerd op het gerechtvaardigd belang van Stichting SKOPOS;
de (categorieën) ontvangers van de persoonsgegevens, zoals verwerkers of derden;
in voorkomend geval: of de persoonsgegevens worden verzonden aan landen buiten de Europese Economische Ruimte (EER);
hoe lang de persoonsgegevens zullen worden bewaard;
dat de betrokkene het recht heeft om Stichting SKOPOS te verzoeken om inzage, verbetering of verwijdering van persoonsgegevens, en dat hij het recht heeft om te verzoeken om beperking van de verwerking, om bezwaar te maken of om een beroep te doen op het recht van gegevensoverdraagbaarheid;
dat de betrokkene het recht heeft om zijn toestemming in te trekken, als de gegevensverwerking is gebaseerd op toestemming;
dat de betrokkene het recht heeft om een klacht in te dienen bij de Autoriteit Persoonsgegevens;
of de verstrekking van de persoonsgegevens een wettelijke of contractuele verplichting is, dan wel een noodzakelijke voorwaarde is om een overeenkomst te kunnen sluiten, en of de betrokkene verplicht is om de persoonsgegevens te verstrekken en wat de gevolgen zijn indien hij de persoonsgegevens niet verstrekt;
het bestaan van eventuele geautomatiseerde besluitvorming, vergezeld van nuttige informatie over de onderliggende logica, alsmede het belang en de verwachte gevolgen van die verwerking voor de betrokkene.

Hoofdstuk 7: Rol (Gemeenschappelijke) Medezeggenschapsraad

De gemeenschappelijke medezeggenschapsraden binnen Stichting SKOPOS hebben op grond van de Wet medezeggenschap op scholen instemmingsrecht over een regeling met betrekking tot de verwerking of de bescherming van persoonsgegevens. Meer specifiek hebben de oudergeledingen instemmingsrecht inzake regelingen over de verwerking van leerlinggegevens of gegevens van ouders en de personeelsgeledingen hebben instemmingsrecht inzake regelingen over de verwerking van gegevens van medewerkers.

Naast de GMR-en is de MR van iedere school een goede partner voor directie en team om te bespreken op welke wijze de school de privacybescherming vorm geeft. Zij hebben adviesrecht als er veranderingen van dit beleid.

Hoofdstuk 8: Specifieke onderwerpen

8.1. Gebruik beeldmateriaal (foto's en video's).

Om deze gegevens van leerlingen te mogen publiceren is meestal toestemming van de ouders en/of verzorgers vereist. Stichting SKOPOS heeft het toestemmingsformulier aangepast aan de AVG en de informatie van de Autoriteit Persoonsgegevens hierover. Dit formulier bevindt zich in **bijlage 7** bij dit IBP-beleid. Iedere school zal jaarlijks toestemming vragen voor bepaalde verwerkingen van het genoemde beeldmateriaal aan de hand van dit formulier en zal ervoor zorgdragen dat er geen beeldmateriaal van leerlingen wordt verwerkt waarvoor geen toestemming is verkregen.

8.2. Email en telefoonnummers.

Voor sociale doeleinden wordt ook toestemming gevraagd voor het verspreiden van leerlingenlijsten. Hierop staan emailadressen en telefoonnummers. Hiervoor wordt éénmalig toestemming gevraagd. Zie **bijlage 8**. (Deze toestemming kan ook reeds zijn opgenomen in het aanmeldformulier).
Voor uitwisseling van persoonsgegevens voor onderwijsdoeleinden hoeft geen toestemming te worden gevraagd. Hiervoor geldt namelijk een wettelijke plicht.

8.3. Privacy bij extra begeleiding en zorg

Stichting SKOPOS kan voor de begeleiding van leerlingen en ouders/verzorgers samenwerken met partners. Daarbij kunnen (bijzondere) persoonsgegevens worden gedeeld. Voor de verwerking van bijzondere persoonsgegevens bestaat een verbod, tenzij daar een wettelijke uitzondering voor bestaat. Zo mogen gegevens over de gezondheid van leerlingen door school worden verwerkt indien dat noodzakelijk is voor de speciale begeleiding van leerlingen of voor het treffen van bijzondere voorzieningen in verband met hun gezondheidstoestand (artikel 30 lid 2 UAVG). Bijvoorbeeld in geval van specifieke beperkingen, epilepsie of ernstige allergieën, dan wel extra begeleiding in verband met dyslexie. Het bestuur sluit aan bij het privacybeleid van het Samenwerkingsverband Passend Onderwijs.

8.4. Privacy bij overstapdossiers

In de wet is het belangrijkste uitgangspunt dat scholen altijd vooraf aan de uitwisseling moeten afwegen welke specifieke gegevens van iedere leerling daadwerkelijk nodig zijn ten behoeve van het leren en begeleiden van een leerling bij een nieuwe organisatie. Dit betekent dat er per leerling die overstapt, moet worden bepaald welke gegevens relevant en proportioneel zijn. Gegevens die niet aan dit criterium voldoen, mogen niet door scholen uitgewisseld worden (hoe handig het doorgeven van die informatie ook lijkt). Welke gegevens dit zijn, is afgesproken en vastgelegd binnen Stichting SKOPOS.
Uitgangspunt: alleen opnemen wat wettelijk verplicht is. Zie **bijlage 10**.
In het "Besluit uitwisseling leer- en begeleidingsgegevens" is namelijk bepaald welke gegevens mogen worden opgenomen in het onderwijskundig rapport. Deze regels en de beperkte set gegevens die volgens dit Besluit mogen worden uitgewisseld vormen de basisvoorwaarde voor een transparante elektronische uitwisseling van gegevens tussen scholen, waarbij de kans op fouten zo klein mogelijk is en de privacy van de betrokkenen gewaarborgd is.
Ook zijn de onderwijswetten van toepassing. In artikel 42 van de Wet op het primair onderwijs is vastgesteld dat een directeur van een school verplicht is om een onderwijskundig rapport op te stellen en te verstrekken aan de nieuwe school. Ook moeten de ouders/ verzorgers een afschrift krijgen. Bezwaren van ouders en/of verzorgers zullen opgenomen moeten worden.

Het bestuur draagt er zorg voor dat alle schooldirecteuren op de hoogte zijn van deze regels.

Hoofdstuk 9: Evaluatie en wijzigingen

9.1. Afspraken over evaluatiemomenten en doorvoeren wijzigingen

Dit IBP-beleid wordt minimaal elke twee jaar in het kader van de Risico-Inventarisatie en Evaluatie (RI&E) getoetst door de FG en worden bijgesteld door de privacycoördinator. De AVG is een apart onderdeel binnen de RI&E. Hierbij wordt rekening gehouden met:

- De status van de informatiebeveiliging als geheel (beleid, organisatie, risico's);
- de actuele geïnventariseerde risico's;
- de effectiviteit van de genomen maatregelen en aantoonbare werking daarvan.

Indien nodig zal het IBP-beleid worden aangepast. Bij substantiële aanpassingen zal het aangepaste IBP-beleid ter goedkeuring worden voorgelegd aan de GMR. Daarnaast kent Stichting SKOPOS een jaarlijkse planning en control cyclus voor informatiebeveiliging en privacy op bestuursniveau. Dit is een periodiek evaluatieproces waarmee de inhoud en effectiviteit van het IBP-beleid wordt getoetst. Ook worden hier actuele ontwikkelingen op het gebied van techniek, wet- en regelgeving en andere relevante ontwikkelingen meegenomen.
Deze jaarlijkse evaluatie vindt plaats in samenspraak met het privacyteam.

9.2. Naleving en sancties

De naleving bestaat uit algemeen toezicht in de dagelijkse praktijk op de naleving van beleid en richtlijnen. Daarnaast wordt er tweejaarlijks een 'Checklist AVG' ingevuld op schoolniveau en op bestuursniveau. Van belang hierbij is dat iedereen zijn verantwoordelijkheid neemt en anderen aanspreekt in geval van tekortkomingen. Er wordt actief aandacht besteed aan IBP bij de aanstelling, tijdens functioneringsgesprekken, met periodieke bewustwordingscampagnes, et cetera.
Voor toezicht op de naleving van de AVG vervult de Functionaris voor Gegevensbescherming (FG) een belangrijke rol. Mocht de naleving van dit IBP-beleid ernstig tekortschieten, dan kan het bestuur de betrokken verantwoordelijke medewerkers een sanctie opleggen binnen de kaders van de CAO en de wettelijke mogelijkheden.

Bijlage 1: Privacyreglement en Privacyverklaring

Privacyreglement voor Stichting SKOPOS

1. Toepasselijkheid	Dit reglement geldt voor de gehele organisatie van Stichting SKOPOS. Stichting SKOPOS is gevestigd op Spoorlaan 60, 5481 SK Schijndel.
2. Definities	
Persoonsgegevens	Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ('de betrokkene'), zoals bijvoorbeeld naam, adres, geboortedatum, titel(s), geslacht, adres, telefoonnummer, e-mailadres, functie, personeelsnummer, medische rapportages, inhoud van e-mails, prestaties/cijfers, brieven, klachten, foto's, video's, IP-adressen, tracking cookies, loginnamen en wachtwoorden.
Verwerking van persoonsgegevens	Een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, geautomatiseerd of handmatig, zoals het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens.
Bijzondere persoonsgegevens	Persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen of het lidmaatschap van een vakbond blijken, genetische gegevens (DNA/RNA) of biometrische gegevens (bijv. foto's) met het oog op de unieke identificatie van een persoon, en gegevens over gezondheid, of iemands seksueel gedrag of seksuele gerichtheid.
Betrokkene	Degene op wie een persoonsgegeven betrekking heeft, en die al dan niet wordt vertegenwoordigd door een wettelijk vertegenwoordiger. Betrokkenen kunnen bijvoorbeeld zijn: leerlingen, ouders, medewerkers en bezoekers.
Wettelijk vertegenwoordiger	Degene die het ouderlijk gezag over een minderjarige uitoefent. Meestal zal dit een ouder zijn, maar het kan ook gaan om een voogd. Als een leerling 16 jaar of ouder is, beslist hij in voorkomende gevallen zelf over zijn privacy.
Verwerkingsverantwoordelijke	De entiteit die het doel en de middelen voor de verwerking van persoonsgegevens vaststelt. In het kader van dit reglement Stichting SKOPOS de verwerkingsverantwoordelijke.
Verwerker	De natuurlijke persoon of rechtspersoon die ten behoeve van de verwerkingsverantwoordelijke (Stichting SKOPOS) persoonsgegevens verwerkt, zoals bijvoorbeeld de leverancier van een leerlingvolgsysteem of leerling-administratiesysteem. Een verwerker heeft een uitvoerende taak, ten behoeve van de activiteiten van de verwerkingsverantwoordelijke.
Derde	Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, niet zijnde de betrokkene, de verwerkingsverantwoordelijke, de verwerker, of de personen die onder rechtstreeks gezag van de verwerkingsverantwoordelijke of de verwerker gemachtigd zijn om persoonsgegevens te verwerken.
Stichting SKOPOS	Stichting SKOPOS, de verwerkingsverantwoordelijke in de zin van dit reglement.

3. Reikwijdte en doelstelling	1. Dit reglement stelt regels over de verwerking van persoonsgegevens van alle betrokkenen bij de organisatie, waaronder leerlingen en hun wettelijk vertegenwoordigers, medewerkers, bezoekers en externe relaties (bijv. leveranciers en opdrachtnemers). 2. Dit reglement is van toepassing op alle persoonsgegevens van de betrokkene die door Stichting SKOPOS worden verwerkt. Het reglement heeft tot doel: a. de persoonlijke levenssfeer van de betrokkenen te beschermen tegen verkeerd en onbedoeld gebruik van de persoonsgegevens; b. vast te stellen met welk doel en op welke (juridische) grondslag persoonsgegevens binnen Stichting SKOPOS worden verwerkt; c. ook overigens te borgen dat persoonsgegevens binnen Stichting SKOPOS rechtmatig, transparant en behoorlijk worden verwerkt; d. de rechten van betrokkenen vast te leggen en te borgen dat deze rechten door Stichting SKOPOS worden gerespecteerd.
4. Doelen van de verwerking van persoonsgegevens	Bij de verwerking van persoonsgegevens houdt Stichting SKOPOS zich aan de relevante wet- en regelgeving waaronder de Algemene Verordening Gegevensbescherming (AVG), de uitvoeringswet AVG en de onderwijswetgeving.
Doelen	1. De verwerking van persoonsgegevens vindt plaats voor: a. de organisatie of het geven van het onderwijs, de begeleiding van leerlingen, het voorzien in hun (extra) ondersteuningsbehoefte, dan wel het geven van studieadviezen; b. het verstrekken en/of ter beschikking stellen van leermiddelen; c. het bewaken van de veiligheid binnen de scholen en het beschermen van eigendommen van medewerkers, leerlingen en bezoekers; d. het bekend maken van informatie over de organisatie en leermiddelen als bedoeld, onder a en b, alsmede van informatie over de leerlingen op de eigen website; e. het bekend maken van de activiteiten van de organisatie, bijvoorbeeld op de website van Stichting SKOPOS of van de scholen, in brochures, ouderbrieven, de schoolgids of via social media; f. het berekenen, vastleggen en innen van inschrijvingsgelden, school- en lesgelden en bijdragen of vergoedingen voor leermiddelen en buitenschoolse activiteiten, waaronder begrepen het in handen van derden stellen van vorderingen; g. het aanvragen van bekostiging, het behandelen van geschillen daarover en het doen uitoefenen van accountantscontrole; h. het onderhouden van contacten met oud-leerlingen; i. het aangaan en uitvoeren van arbeidsovereenkomsten, samenwerkingsrelaties met opdrachtnemers en contracten met leveranciers; j. de uitvoering of toepassing van wet- en regelgeving; k. juridische procedures waarbij Stichting SKOPOS betrokken is. 2. De verwerking van persoonsgegevens mag ook plaatsvinden voor doelen die verenigbaar zijn met de doelen zoals beschreven in lid 1.
5. Doelbinding	Persoonsgegevens worden uitsluitend gebruikt voor zover dat gebruik verenigbaar is met de omschreven doelen van de verwerking. Stichting SKOPOS verwerkt niet meer gegevens dan noodzakelijk is om de betreffende doelen te bereiken. Persoonsgegevens worden alleen verwerkt daar waar dat strikt noodzakelijk is voor de uitvoering van vooraf duidelijk bepaalde en uitdrukkelijk omschreven gerechtvaardigde doelen op basis van de grondslagen zoals beschreven in de wet. Doelen zijn voordat de verwerking plaatsvindt concreet en specifiek geformuleerd. Persoonsgegevens worden niet verder verwerkt voor

	andere doelen die hiermee onverenigbaar zijn. Het omschreven doel vormt een kader waaraan kan worden getoetst of de verwerking van de gegevens noodzakelijk is voor dat doel en/of verenigbaar is met een ander doel.
6. Verdere verwerkingen	Indien er sprake is van verdere (secundaire) verwerking van persoonsgegevens (bijv. voor het doel van (wetenschappelijk) onderzoek), dient te worden nagegaan of deze secundaire verwerking verenigbaar is met de doeleinden waarvoor de persoonsgegevens oorspronkelijk verzameld werden. Betrokkenen dienen omtrent deze verdere (secundaire) verwerking van hun persoonsgegevens geïnformeerd te worden.
7. Soorten persoonsgegevens	De categorieën van persoonsgegevens zoals deze binnen Stichting SKOPOS worden verwerkt, worden geregistreerd in een verwerkingsregister.
8. Grondslag verwerking	Verwerking van persoonsgegevens gebeurt alleen indien aan een van de onderstaande voorwaarden is voldaan: a. De verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan Stichting SKOPOS is opgedragen. b. De verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op Stichting SKOPOS rust. c. De verwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is (bijvoorbeeld de arbeidsovereenkomst) of om op verzoek van de betrokkene vóór de sluiting van een overeenkomst maatregelen te nemen. d. De verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van Stichting SKOPOS of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene zwaarder wegen, met name wanneer de betrokkene een kind is; in het kader van deze grondslag zal dus een belangenafweging moeten plaatsvinden. e. De verwerking is noodzakelijk om de vitale belangen van de betrokkene of een andere natuurlijke persoon te beschermen (levensbelang). f. De betrokkene heeft toestemming gegeven voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden.
9. Bewaartermijnen	Stichting SKOPOS bewaart persoonsgegevens niet langer dan noodzakelijk is voor het doel waarvoor deze worden verwerkt, tenzij het langer bewaren van de persoonsgegevens op grond van wet- of regelgeving verplicht is. Binnen Stichting SKOPOS geldt dat personen slechts toegang hebben tot persoonsgegevens voor zover dat daadwerkelijk nodig is. De toegang van medewerkers tot persoonsgegevens is dan ook beperkt tot de gegevens die noodzakelijk zijn voor de goede uitoefening van hun functie en (dus) hun werkzaamheden. Verder wordt slechts toegang verschaft tot de in de administratie en systemen van de school opgenomen persoonsgegevens aan: a. De verwerker die van Stichting SKOPOS de opdracht heeft gekregen om persoonsgegevens te verwerken, maar alleen voor zover dat noodzakelijk is in het licht van de gemaakte afspraken; b. Derden voor zover uit de wet voortvloeit dat Stichting SKOPOS verplicht is om toegang te geven of sprake is van een (andere) grondslag voor deze verwerking, bijvoorbeeld de vervulling van een taak van algemeen belang.

10. Beveiliging en geheimhouding	1. Stichting SKOPOS neemt passende technische en organisatorische beveiligingsmaatregelen om te voorkomen dat de persoonsgegevens (zowel digitaal als op papier) worden beschadigd, verloren gaan of onrechtmatig worden verwerkt. Deze maatregelen zijn er mede op gericht om niet noodzakelijke verzameling en verdere (niet noodzakelijke) verwerking van persoonsgegevens te voorkomen. 2. Bij de beveiligingsmaatregelen wordt rekening gehouden met de stand van de techniek, de uitvoeringskosten, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van betrokkenen. 3. Eenieder die betrokken is bij de verwerking van persoonsgegevens binnen Stichting SKOPOS is verplicht tot geheimhouding van de betreffende persoonsgegevens, en zal deze gegevens slechts verwerken voor zover dat noodzakelijk is voor de uitoefening van de betreffende functie, werkzaamheden of taak.
11. Verstrekken gegevens aan derden	Stichting SKOPOS deelt persoonsgegevens niet zomaar met derden. Dat doet Stichting SKOPOS wel als de betrokkene daarvoor toestemming heeft gegeven, als Stichting SKOPOS daartoe verplicht is op grond van de wet, als dat nodig is voor de uitvoering van een overeenkomst waarbij betrokkene partij is, of als Stichting SKOPOS daartoe een gerechtvaardigd belang heeft. In sommige gevallen deelt Stichting SKOPOS persoonsgegevens wel met derden. Deze derde partijen kwalificeren alsdan als verwerker in de zin van de AVG en Stichting SKOPOS als verwerkingsverantwoordelijke. Met derde partijen aan wie Stichting SKOPOS persoonsgegevens verstrekt en die onder de verantwoordelijkheid van Stichting SKOPOS persoonsgegevens verwerken, sluit Stichting SKOPOS een schriftelijke overeenkomst, de verwerkersovereenkomst. In deze overeenkomst worden afspraken gemaakt ter bescherming van de persoonsgegevens. Zo zorgt Stichting SKOPOS ervoor dat derde partijen voor doelen en onder voorwaarden die Stichting SKOPOS met hen heeft afgesproken, persoonsgegevens verwerkt. Als Stichting SKOPOS samenwerkt met ZZP'ers, tijdelijke krachten of partners die geen verwerkers zijn omdat ze onder direct gezag van Stichting SKOPOS staan, en het is noodzakelijk om persoonsgegevens uit te wisselen, sluit Stichting SKOPOS een geheimhoudingsovereenkomst.
12. Verwerking buiten de EU/EER	De persoonsgegevens worden niet getransfereerd en verwerkt naar derde landen (buiten de EU/EER). De verwerkers van ORGANISATIE zijn afkomstig uit de Europese Unie, of hebben een relevante vestiging in de EU, waardoor ze zich aan de AVG moeten houden. ORGANISATIE geeft dus géén persoonsgegevens door naar landen waar persoonsgegevens minder goed worden beschermd. Indien er in afwijking van deze hoofdregel toch sprake is van doorgifte van persoonsgegevens naar derde landen (buiten de EU/EER), dan zal deze doorgifte uitsluitend plaatsvinden als dit derde land voldoende bescherming biedt. Deze bescherming kan worden geboden op basis van een adequaatheidsbesluit, passende waarborgen, bindende bedrijfsvoorschriften (BCR) of specifieke uitzonderingen, zoals beschreven in de AVG.
13. Sociale media	Voor het gebruik van persoonsgegevens in sociale media, zijn aparte afspraken gemaakt in het sociale mediaprotocol van Stichting SKOPOS.

14. Rechten betrokkenen	1. Stichting SKOPOS erkent de rechten van betrokkenen, handelt daarmee in overeenstemming en bewerkstelligt dat betrokkenen deze rechten daadwerkelijk kunnen uitoefenen. Het betreft in het bijzonder de volgende rechten:
Inzage	Een betrokkene heeft recht op inzage van de door Stichting SKOPOS verwerkte persoonsgegevens die op hem betrekking hebben, behalve voor zover het gaat om interne notities, die uitsluitend bedoeld zijn voor intern overleg en beraad. Indien en voor zover dit recht op inzage ook de rechten en vrijheden van anderen raakt, bijvoorbeeld als in de documenten ook persoonsgegevens van anderen dan de betrokkene zijn vermeld, kan Stichting SKOPOS het recht op inzage beperken. Bij het verstrekken van de betreffende gegevens verschaft Stichting SKOPOS voorts informatie over: de verwerkingsdoeleinden; de categorieën van persoonsgegevens die worden verwerkt; de ontvangers of categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt; (indien van toepassing) ontvangers in derde landen of internationale organisaties; (indien mogelijk) hoe lang de gegevens worden bewaard; dat de betrokkene het recht heeft om te verzoeken dat de persoonsgegevens worden gerectificeerd of gewist, of dat de verwerking van de persoonsgegevens wordt beperkt, alsmede dat hij het recht heeft om bezwaar te maken tegen de verwerking van de persoonsgegevens; het feit dat de betrokkene een klacht kan indienen bij de Autoriteit Persoonsgegevens; de bron van de persoonsgegevens, indien de persoonsgegevens niet van de betrokkene zelf zijn verkregen; het eventueel toepassen van geautomatiseerde besluitvorming en de betreffende onderliggende logica en het belang en de gevolgen voor de betrokkene; de passende waarborgen indien de persoonsgegevens worden doorgegeven aan een derde land of een internationale organisatie.
Verbetering, aanvulling, verwijdering	Stichting SKOPOS verbetert de persoonsgegevens van een betrokkene in het geval de betrokkene terecht heeft aangegeven dat de gegevens onjuist zijn, en Stichting SKOPOS vult de persoonsgegevens van een betrokkene aan indien de betrokkene terecht om aanvulling heeft verzocht. Voorts kan de betrokkene verzoeken om verwijdering van zijn persoonsgegevens. Stichting SKOPOS gaat daartoe over indien is voldaan aan een wettelijke grondslag voor het verzoek, tenzij het onmogelijk is om aan het verzoek te voldoen of dit een onredelijke inspanning zou vergen.
Bezwaar	Indien Stichting SKOPOS persoonsgegevens verwerkt op de grondslag van artikel 7 onder a of artikel 7 onder d van dit reglement, kan het betrokkene bezwaar maken tegen de verwerking van zijn persoonsgegevens. In dat geval staakt Stichting SKOPOS de verwerking van de betreffende persoonsgegevens, behalve als naar het oordeel van Stichting SKOPOS, het belang van derden of het algemeen belang in het betreffende concrete geval zwaarder weegt.
Beperken verwerking	De betrokkene kan voorts verzoeken om de verwerking van zijn persoonsgegevens te beperken, namelijk indien hij een verzoek tot verbetering heeft gedaan, indien hij bezwaar heeft gemaakt tegen de verwerking, als de persoonsgegevens niet meer nodig zijn voor het doel van de verwerking of als de gegevensverwerking onrechtmatig is. Stichting SKOPOS staakt dan de verwerking, tenzij de betrokkene toestemming heeft gegeven voor de verwerking, de gegevens nodig zijn

	voor een rechtszaak of de verwerking nodig is ter bescherming van de rechten van een andere persoon of vanwege gewichtige redenen.
Kennisgevingsplicht	Als Stichting SKOPOS op verzoek van een betrokkene een verbetering of verwijdering van persoonsgegevens heeft uitgevoerd, of de verwerking van persoonsgegevens heeft beperkt, zal Stichting SKOPOS eventuele ontvangers van de betreffende persoonsgegevens daarover informeren.
Procedure	2. Stichting SKOPOS handelt een verzoek van een betrokkene zo spoedig mogelijk, maar uiterlijk binnen een maand na ontvangst van het verzoek, af. Afhankelijk van de complexiteit en van het aantal verzoeken kan die termijn indien nodig met twee maanden worden verlengd. Als deze verlenging plaatsvindt, wordt de betrokkene daarover binnen een maand na de ontvangst van het verzoek geïnformeerd. Wanneer de betrokkene zijn verzoek elektronisch indient, wordt de informatie indien mogelijk elektronisch verstrekt, tenzij de betrokkene anderszins verzoekt. Wanneer Stichting SKOPOS geen gevolg geeft aan het verzoek van de betrokkene, deelt Stichting SKOPOS onverwijld en uiterlijk binnen een maand na ontvangst mede waarom het verzoek niet wordt ingewilligd en informeert hij de betrokkene over de mogelijkheid om een klacht in te dienen bij de Autoriteit Persoonsgegevens of beroep bij de rechter in te stellen.
Intrekken toestemming	3. Indien voor de verwerking van persoonsgegevens voorafgaande toestemming vereist is, kan deze toestemming te allen tijde door de betrokkene of zijn wettelijk vertegenwoordiger worden ingetrokken. Als de toestemming wordt ingetrokken, staakt Stichting SKOPOS de verwerking van persoonsgegevens, behalve als er een andere grondslag (zoals bedoeld in artikel 7) voor de gegevensverwerking is. Het intrekken van de toestemming tast de rechtmatigheid van verwerkingen die reeds hebben plaatsgevonden niet aan.
15. Transparantie	Stichting SKOPOS informeert de betrokkene(n) actief over de verwerking van hun persoonsgegevens, in ieder geval door middel van een laagdrempelige privacyverklaring. In de privacyverklaring wordt in ieder geval de volgende informatie vermeld: a. de contactgegevens van Stichting SKOPOS; b. de contactgegevens van de functionaris voor gegevensbescherming van Stichting SKOPOS; c. de doeleinden van de gegevensverwerking en de grondslagen voor de verwerking; d. een omschrijving van de belangen van Stichting SKOPOS indien de verwerking wordt gebaseerd op het gerechtvaardigd belang van Stichting SKOPOS; e. de (categorieën) ontvangers van de persoonsgegevens, zoals verwerkers of derden; f. in voorkomend geval: of de persoonsgegevens worden verzonden aan landen buiten de Europese Economische Ruimte (EER); g. hoe lang de persoonsgegevens zullen worden bewaard; h. dat de betrokkene het recht heeft om Stichting SKOPOS te verzoeken om inzage, verbetering of verwijdering van persoonsgegevens, en dat hij het recht heeft om te verzoeken om beperking van de verwerking, om bezwaar te maken of om een beroep te doen op het recht van gegevensoverdraagbaarheid; i. dat de betrokkene het recht heeft om zijn toestemming in te trekken, als de gegevensverwerking is gebaseerd op toestemming; j. dat de betrokkene het recht heeft om een klacht in te dienen bij de Autoriteit Persoonsgegevens;

	k. of de verstrekking van de persoonsgegevens een wettelijke of contractuele verplichting is, dan wel een noodzakelijke voorwaarde is om een overeenkomst te kunnen sluiten, en of de betrokkene verplicht is om de persoonsgegevens te verstrekken en wat de gevolgen zijn indien hij de persoonsgegevens niet verstrekt; l. het bestaan van geautomatiseerde besluitvorming, vergezeld van nuttige informatie over de onderliggende logica, alsmede het belang en de verwachte gevolgen van die verwerking voor de betrokkene.
16. Meldplicht datalekken	Eenieder die betrokken is bij een verwerking van persoonsgegevens is verplicht om een datalek per ommegaande te melden bij het meldpunt (privacy@skoposschijndel.nl) conform het protocol beveiligingsincidenten en datalekken van Stichting SKOPOS. Een datalek is elke inbreuk waarbij persoonsgegevens zijn vernietigd of verloren, gewijzigd, verstrekt of toegankelijk zijn gemaakt. Bijvoorbeeld door het laten rondslingeren van wachtwoorden, usb-stick/ externe harde schijf of lijsten met leerlinggegevens.
17. Klachten	a. Wanneer een betrokkene van mening is dat het doen of nalaten van Stichting SKOPOS niet in overeenstemming is met de AVG, dit reglement of (andere) toepasselijke wet- of regelgeving, dan kan een klacht worden ingediend overeenkomstig de binnen Stichting SKOPOS geldende klachtenregeling. Een betrokkene kan zich eveneens wenden tot de functionaris voor gegevensbescherming van Stichting SKOPOS. b. Als een klacht naar de mening van betrokkene door Stichting SKOPOS niet correct is afgewikkeld, kan hij zich wenden tot de rechter of de Autoriteit Persoonsgegevens.
18. Onvoorziene situatie	Indien zich een situatie voordoet die niet beschreven is in dit reglement, neemt Stichting SKOPOS de benodigde maatregelen, en wordt beoordeeld of dit reglement dientengevolge moet worden aangevuld of aangepast.
19. Wijzigingen reglement	a. Dit reglement is na instemming van de Gemeenschappelijke Medezeggenschapsraad (GMR) vastgesteld door het bestuur van Stichting SKOPOS. Het reglement wordt gepubliceerd op de website van Stichting SKOPOS en de websites van de scholen. Het reglement wordt verder actief onder de aandacht gebracht, bijvoorbeeld door middel van verwijzing in de schoolgids. b. Het bestuur kan dit reglement wijzigen na instemming van de GMR.
20. Slotbepaling	Dit reglement wordt aangehaald als het privacyreglement van Stichting SKOPOS en treedt in werking op 1 maart 2023.

skopos

Privacyverklaring voor ouders

Stichting SKOPOS en de Algemene Verordening Gegevensbescherming (AVG).

Contactgegevens: Stichting SKOPOS, Spoorlaan 60, 5481 SK Schijndel
Contactgegevens Functionaris voor Gegevensbescherming: fg@lumengroup.nl

Onze scholen verwerken persoonsgegevens van u en uw kinderen. Stichting SKOPOS is als stichting wettelijk verantwoordelijk. Stichting SKOPOS vindt een goede omgang met persoonsgegevens van groot belang en is zich bewust van de privacywetgeving. We leggen u graag uit hoe wij met de persoonsgegevens van uw kind omgaan.

Waarom verwerken wij gegevens van uw kind?
Wij verwerken persoonsgegevens op basis van een van de volgende grondslagen:

- De verwerking is noodzakelijk om te voldoen aan een wettelijke plicht die op Stichting SKOPOS rust. Stichting SKOPOS verwerkt persoonsgegevens van leerlingen om onze verplichtingen als onderwijsinstelling te kunnen nakomen. Zo hebben wij bijvoorbeeld de gegevens nodig om leerlingen aan te melden als leerling op onze school en om de voortgang bij te houden. Daarnaast hebben wij de wettelijke verplichting om bepaalde gegevens door te sturen naar andere partijen, zoals DUO (ministerie van Onderwijs) en leerplicht.
- De verwerking van de gegevens dient een algemeen belang.
- De verwerking is noodzakelijk ter uitvoering van een overeenkomst.
- Na toestemming van de leerling of ouders van de leerlingen jonger dan 16 jaar. Een eenmaal gegeven toestemming mag op ieder moment weer worden ingetrokken, zonder opgaaf van reden.
- De verwerking is noodzakelijk om de vitale belangen van de leerling te beschermen (levensbelang).
- De verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van Stichting SKOPOS. Hiervoor wordt per specifiek geval een belangenafweging gemaakt.

Welke gegevens verwerken wij van uw kind?
Wij verwerken diverse soorten gegevens, waarvan wij de meeste gegevens rechtstreeks van u als ouders hebben gekregen. U kunt hierbij denken aan contactgegevens en geboorteplaats. Als u weigert de voor ons noodzakelijke gegevens te verstrekken, kunnen wij onze verplichtingen niet nakomen. De verstrekking van deze gegevens is dan ook een voorwaarde om uw kind bij ons in te kunnen schrijven. Wij verwerken ook medische gegevens van leerlingen indien dat noodzakelijk is voor de juiste onderwijskundige, specifieke begeleiding. Ook verwerken wij medische gegevens als die nodig zijn om in noodgevallen goed te kunnen handelen.

Welke persoonsgegevens wij van uw kind verwerken voor welke doeleinden vindt u hieronder:

Categorie	Doeleinden
1. Contactgegevens	1a: naam, voornaam, e-mail, opleiding; 1b: geboortedatum, geslacht; 1c: overige gegevens te weten: adres, postcode, woonplaats, telefoonnummer en eventueel andere voor communicatie benodigde gegevens, alsmede ook een bankrekeningnummer voor het afhandelen van betalingen.
2. Leerlingnummer	Een administratienummer dat geen andere informatie bevat dan bedoeld onder categorie 1.
3. Nationaliteit en geboorteplaats	Gegevens die noodzakelijk zijn met het oog op de gezondheid of het welzijn van de leerling, voor zover deze van belang zijn bij het nemen van aanvullende maatregelen om goed onderwijs te kunnen volgen.
4. Ouders, voogd	Contactgegevens van de ouders/verzorgers van leerlingen (naam, voornaam, adres, postcode, woonplaats, telefoonnummer en eventueel e-mailadres).
5. Medische gegevens	Gegevens die noodzakelijk zijn met het oog op de gezondheid of het welzijn van de leerling, voor zover deze van belang zijn bij het nemen van aanvullende maatregelen om goed onderwijs te kunnen volgen.

6. Godsdienst	Gegevens betreffende de godsdienst of levensovertuiging van de leerling, voor zover die noodzakelijk zijn voor het te volgen onderwijs (bijvoorbeeld: leerling vrij op bepaalde dag).
7. Voortgang	Gegevens betreffende de aard en het verloop van het onderwijs en de behaalde studieresultaten te weten: • Toetsen • Begeleiding leerling (inclusief ontwikkelperspectief OPP) • Aanwezigheidsregistratie • Medisch dossier • Klas/groep, leerjaar
8. Onderwijsorganisatie	Gegevens met het oog op het organiseren van het onderwijs en het verstrekken of ter beschikking stellen van leermiddelen.
9. Financiën	Gegevens voor het berekenen, vastleggen en innen van bijdragen of vergoedingen voor leermiddelen en buitenschoolse activiteiten (denk hierbij aan een bankrekeningnummer van de ouders).
10. Beeldmateriaal	Foto's en videobeelden (met of zonder geluid) van activiteiten van de school op basis van toestemming. Let op: Voor pasfoto voor identificatiedoeleinden is geen toestemming nodig; Als aanvulling op het dossier.
11. Leraar /zorgcoördinator/ intern begeleider	Gegevens van leraren en begeleiders, voor zover deze gegevens van belang zijn voor de organisatie van de instelling en het geven van onderwijs.
12. BSN (PGN)	In het onderwijs heet het BSN het persoonsgebonden nummer (PGN). Ook wel onderwijsnummer genoemd. Het PGN is hetzelfde nummer als het BSN. Scholen zijn verplicht het PGN te gebruiken in hun administratie.
13. Keten-ID (Eck-Id)	Unieke ID voor de 'educatieve contentketen'. Hiermee kunnen scholen gegevens delen, zonder dat ze direct herleidbaar zijn naar leerlingen of leraren. Is dit ook geen wettelijke plicht hiervan gebruik te maken als schoolorganisatie?
14 Overige gegevens, te weten …	Andere dan de onder 1 tot en met 11 bedoelde gegevens waarvan de verwerking wordt vereist of noodzakelijk is met het oog op de toepassing van een andere wet. Deze zullen apart vermeld en toegelicht worden.

Hoe gaan wij om met de gegevens van uw kind?
Bij het verwerken van de gegevens gaan wij altijd uit van noodzakelijkheid, wij zullen niet meer gegevens verwerken dan noodzakelijk is om onze rechten en plichten als onderwijsinstelling na te komen. Dit betekent ook dat we de gegevens niet zullen gebruiken voor andere doeleinden dan wij in deze toelichting noemen.

Wij zullen de gegevens van uw kind niet delen met commerciële derde partijen voor andere doeleinden. Ook zullen wij de gegevens van uw kind nooit verkopen of verhuren aan derde partijen. 'Verdere verwerking' betreft alle verwerkingen van persoonsgegevens voor een ander doel dan waarvoor de persoonsgegevens oorspronkelijk zijn verzameld. Dit kan een verwerking door ons als organisatie zijn, maar kan ook de basis zijn voor verstrekking van gegevens aan een andere verwerkingsverantwoordelijke. Dit doen we enkel wanneer het verstrekken van de persoonsgegevens verenigbaar is met het doel waarvoor de gegevens in eerste instantie zijn verzameld.

De persoonsgegevens worden zoveel mogelijk gecodeerd bewaard en alleen die medewerkers kunnen bij de gegevens, die dat ook voor de uitvoering van hun werk nodig hebben. Daarnaast bewaren wij de gegevens niet langer dan noodzakelijk is. Wij hanteren hiervoor verschillende bewaartermijnen die wettelijk geregeld en vastgesteld zijn. Gegevens uit de leerling-administratie worden over het algemeen 5 jaar bewaard.

Welke rechten hebben ouders van leerlingen jonger dan 16 jaar?
Je hebt specifieke rechten ten aanzien van de verwerking van jouw persoonsgegevens. Je hebt de volgende rechten:

- Weten of wij jouw persoonsgegevens verwerken;
- Inzage in de persoonsgegevens die wij van jou verwerken;
- Informatie over de verwerking van jouw persoonsgegevens;

- Bezwaar maken tegen het verwerken van jouw persoonsgegevens;
- Aanpassing van jouw persoonsgegevens als deze (mogelijk) onjuist zijn;
- Aanvulling van jouw persoonsgegevens als deze (mogelijk) onvolledig zijn;
- Beperking van de verwerking van jouw persoonsgegevens;
- Verwijdering (wissen) van jouw persoonsgegevens;
- Overdracht van jouw persoonsgegevens aan jezelf of aan een andere organisatie op jouw verzoek;
- Beantwoording vragen over de inhoud van deze privacyverklaring.

Als je vragen hebt of wilt weten welke persoonsgegevens wij van jou verwerken, kun je altijd contact met ons opnemen (zie de contactgegevens bovenaan deze privacyverklaring). Let op dat je altijd duidelijk aangeeft wie je bent, zodat wij kunnen verifiëren dat jouw verzoek/vraag betrekking heeft op jouw eigen gegevens.

Wij zullen binnen één maand van ontvangst van je verzoek reageren op welke wijze we gevolg hebben gegeven (of gaan geven) aan jouw verzoek. Afhankelijk van de ingewikkeldheid en aantal verzoeken, kan deze termijn met twee maanden worden verlengd. Ook hierover zullen we je binnen één maand na ontvangst informeren.

Stichting SKOPOS zal geen besluiten nemen over uw kind, die alleen gebaseerd zijn op geautomatiseerde verwerking van gegevens. Beslissingen worden nooit zonder menselijke tussenkomst genomen.

Als u het niet eens bent met hoe wij omgaan met de gegevens van uw kind, dan kunt u opheldering vragen bij de directeur van uw school. Als u daarna nog vragen heeft, kunt u onze Functionaris voor Gegevensbescherming benaderen: fg@lumengroup.nl. Indien uw probleem volgens u niet goed wordt opgelost, dan kunt u dat melden bij Autoriteit voor de Persoonsgegevens www.autoriteitpersoonsgegevens.nl.

Hoe beveiligen wij uw gegevens?
Beveiliging van persoonsgegevens is voor ons van groot belang. Wij hebben passende technische en organisatorische maatregelen getroffen om jouw persoonsgegevens te beveiligen. We passen de beveiliging steeds aan en letten goed op om te voorkomen dat er iets mis kan gaan.

- Wachtwoordenbeleid
- Rollen en rechten
- Werken met ZIVVER (beveiligd mailen)
- TLS
- MFA

Aan wie verstrekken wij uw gegevens?
Wij verstrekken jouw persoonsgegevens niet zomaar aan anderen. Dat mogen wij alleen doen als je ons daarvoor toestemming hebt gegeven, als wij daartoe verplicht zijn op grond van de wet, als het nodig is voor de uitvoering van een overeenkomst waarbij jij betrokken bent, of als wij daartoe een gerechtvaardigd belang hebben.

In een aantal gevallen zijn wij, zoals eerder aangegeven, verplicht om gegevens van uw kind te delen met andere organisaties. Dit zijn onder andere DUO, leerplicht, de onderwijsinspectie, GGD/schoolarts, samenwerkingsverband en accountant.

Verwerkers
Met derde partijen aan wie wij jouw persoonsgegevens verstrekken en die onder onze verantwoordelijkheid jouw persoonsgegevens verwerken, sluiten wij schriftelijke overeenkomsten. In deze overeenkomsten worden afspraken gemaakt ter bescherming van jouw persoonsgegevens. Zo zorgen wij er voor dat derde partijen jouw persoonsgegevens alleen verwerken voor de afgesproken doelen en onder vooraf vastgestelde voorwaarden.

Wij kunnen commerciële derde partijen verzoeken om te ondersteunen bij het verwerken van de gegevens voor de eerdergenoemde doeleinden. Denk hierbij aan applicaties om leerlingen in de les te ondersteunen, een administratiesysteem waarbij de gegevens niet op ons eigen netwerk worden opgeslagen, maar bij een andere organisatie of een lesroosterprogramma. Dit gebeurt altijd in opdracht en

onder de verantwoordelijkheid van Stichting SKOPOS. Met deze organisaties sluiten we overeenkomsten af, waarin o.a. is vastgelegd welke gegevens er verwerkt worden en hoe deze gegevens beveiligd worden.

Verwerking van persoonsgegevens buiten de EU/EER
Persoonsgegevens worden NIET door SKOPOS of haar verwerkers buiten de EU/EER verwerkt. Indien dit het geval is, dan dragen wij er zorg voor dat de persoonsgegevens adequaat worden beschermd.

Wijzigingen
Stichting SKOPOS kan dit document aanpassen, bijvoorbeeld als de verwerking van persoonsgegevens wijzigt. De nieuwe versie zal op de website van onze school worden geplaatst.

skopos

Privacyverklaring voor medewerkers

Contactgegevens: Stichting SKOPOS, Spoorlaan 60, 5481 SK Schijndel
Contactgegevens Functionaris voor Gegevensbescherming: fg@lumengroup.nl.

Het bestuur verwerkt uw persoonsgegevens. Stichting SKOPOS is als stichting wettelijk verantwoordelijk. Het bestuur vindt een goede omgang met persoonsgegevens van groot belang en is zich bewust van de privacywetgeving. We leggen u graag uit hoe het bestuur met uw persoonsgegevens omgaat.

Waarom verwerken wij uw gegevens?
Stichting SKOPOS verwerkt persoonsgegevens van medewerkers om de verplichtingen als werkgever te kunnen nakomen. Wij verwerken persoonsgegevens van medewerkers voor de volgende doeleinden:

- Het aangaan en vaststellen van de arbeidsovereenkomst;
- Het uitvoeren van de arbeidsovereenkomst;
- Berekenen en vastleggen van salarissen en andere tegoeden;
- Het betalen van salarissen en andere tegoeden, en de afdracht van premies en belastingen;
- Het verlenen van ontslag;
- Het regelen van en de controle op aanspraken op uitkeringen in verband met de beëindiging van het dienstverband;
- Het geven van leiding en ondersteuning aan de medewerker;
- Het toegang geven tot het bedrijfsnetwerk;
- Om te voldoen aan wettelijke verplichtingen (Belasting, Pensioen, Accountant);
- Het innen van vorderingen;
- Het behandelen van geschillen;
- De behandeling van personeelszaken;
- Het verstrekken van bedrijfs-medische zorg voor de werknemers en het kunnen nakomen van re-integratieverplichtingen bij verzuim;
- Het zorgen voor de veiligheid van werknemers binnen Stichting SKOPOS.

Welke persoonsgegevens wij van u verwerken vindt u hieronder:

Categorie	Doeleinden
1. Contactgegevens	1a: naam, voornaam, e-mail, opleiding; 1b: geboortedatum, geslacht; 1c: overige gegevens te weten: adres, postcode, woonplaats, telefoonnummer en eventueel andere voor communicatie benodigde gegevens, alsmede ook een bankrekeningnummer voor het afhandelen van betalingen.
2. Werknemersnummer	Een administratienummer dat geen andere informatie bevat dan bedoeld onder categorie 1.
3. Nationaliteit en geboorteplaats	Gegevens die noodzakelijk zijn met het oog op de gezondheid of het welzijn van de medewerker.
4. Verzuim- en verlofgegevens	Gegevens die noodzakelijk zijn met het oog op de gezondheid of het welzijn van de medewerker, voor zover deze van belang zijn bij het nemen van aanvullende maatregelen om goed onderwijs te kunnen geven.
5. Professionalisering	Gegevens betreffende de aard en het verloop van het onderwijs en de behaalde studieresultaten te weten: • Diploma's en certificaten • Gevolgde cursussen • Curriculum vitae
6. Financiën	Gegevens voor het berekenen, vastleggen en uitbetalen van salaris of vergoedingen (denk hierbij aan een bankrekeningnummer.
7. BSN (PGN)	Werkgever is verplicht het BSN te gebruiken in hun administratie.

Op basis waarvan verwerken wij jouw gegevens?
Wij verwerken persoonsgegevens op basis van een van de volgende grondslagen:

- De verwerking is noodzakelijk om te voldoen aan een wettelijke plicht die op Stichting SKOPOS rust.
- De verwerking van de gegevens dient een algemeen belang.
- De verwerking is noodzakelijk ter uitvoering van een overeenkomst.
- Na toestemming van de medewerker in kwestie. Een eenmaal gegeven toestemming mag op ieder moment weer worden ingetrokken, zonder opgaaf van reden.
- De verwerking is noodzakelijk om de vitale belangen van de medewerker te beschermen (levensbelang).
- De verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van Stichting SKOPOS. Hiervoor wordt per specifiek geval een belangenafweging gemaakt.

Bij het verwerken van de gegevens gaan wij altijd uit van noodzakelijkheid en proportionaliteit. Stichting SKOPOS zal niet meer gegevens verwerken dan noodzakelijk is en deze persoonsgegevens op de minst ingrijpende manieren verwerken om de rechten en plichten na te komen. Dit betekent ook dat we de gegevens niet zullen gebruiken voor andere doeleinden dan wij in deze toelichting noemen.

Welke rechten hebben medewerkers?
Je hebt specifieke rechten ten aanzien van de verwerking van jouw persoonsgegevens. Je hebt de volgende rechten:

- Weten of wij jouw persoonsgegevens verwerken;
- Inzage in de persoonsgegevens die wij van jou verwerken;
- Informatie over de verwerking van jouw persoonsgegevens;
- Bezwaar maken tegen het verwerken van jouw persoonsgegevens;
- Aanpassing van jouw persoonsgegevens als deze (mogelijk) onjuist zijn;
- Aanvulling van jouw persoonsgegevens als deze (mogelijk) onvolledig zijn;
- Beperking van de verwerking van jouw persoonsgegevens;
- Verwijdering (wissen) van jouw persoonsgegevens;
- Overdracht van jouw persoonsgegevens aan jezelf of aan een andere organisatie op jouw verzoek;
- Beantwoording vragen over de inhoud van deze privacyverklaring.

Als je vragen hebt of wilt weten welke persoonsgegevens wij van jou verwerken, kun je altijd contact met ons opnemen (zie de contactgegevens bovenaan deze privacyverklaring). Let op dat je altijd duidelijk aangeeft wie je bent, zodat wij kunnen verifiëren dat jouw verzoek/vraag betrekking heeft op jouw eigen gegevens.

Wij zullen binnen één maand van ontvangst van je verzoek reageren op welke wijze we gevolg hebben gegeven (of gaan geven) aan jouw verzoek. Afhankelijk van de ingewikkeldheid en aantal verzoeken, kan deze termijn met twee maanden worden verlengd. Ook hierover zullen we je binnen één maand na ontvangst informeren.

Als u ons verzoekt om uw gegevens beperken of te wissen, zullen wij toetsen of dit mogelijk is.
In deze toets houden wij ons aan de wettelijke voorschriften en kijken wij bijvoorbeeld of wij geen wettelijke plicht hebben om de gegevens te bewaren.

Als u het niet eens bent met hoe wij omgaan met uw gegevens, dan kunt u opheldering vragen bij de leidinggevende. Als u daarna nog vragen heeft, kunt u onze Functionaris voor Gegevensbescherming benaderen: fg@lumengroup.nl. Indien uw probleem volgens u niet goed wordt opgelost, dan kunt u dat melden bij Autoriteit voor de Persoonsgegevens www.autoriteitpersoonsgegevens.nl.

Hoe beveiligen wij jouw gegevens?
Beveiliging van persoonsgegevens is voor ons van groot belang. Wij hebben passende technische en organisatorische maatregelen getroffen om jouw persoonsgegevens te beveiligen. We passen de beveiliging steeds aan en letten goed op om te voorkomen dat er iets mis kan gaan.

- Wachtwoordenbeleid
- Rollen en rechten
- Werken met ZIVVER (beveiligd mailen)

- TLS
- MFA

Aan wie verstrekken wij jouw gegevens?
Wij verstrekken jouw persoonsgegevens niet zomaar aan anderen. Dat mogen wij alleen doen als je ons daarvoor toestemming hebt gegeven, als wij daartoe verplicht zijn op grond van de wet, als het nodig is voor de uitvoering van een overeenkomst waarbij jij betrokken bent, of als wij daartoe een gerechtvaardigd belang hebben.

Andere verwerkingsverantwoordelijken
Voor het uitvoeren van de arbeidsovereenkomst en het voldoen aan wettelijke plichten verstrekken we in sommige gevallen werknemersgegevens aan bijvoorbeeld de Belastingdienst, pensioenfondsen en arbodiensten.

Verwerkers
Met derde partijen aan wie wij jouw persoonsgegevens verstrekken en die onder onze verantwoordelijkheid jouw persoonsgegevens verwerken, sluiten wij schriftelijke overeenkomsten. In deze overeenkomsten worden afspraken gemaakt ter bescherming van jouw persoonsgegevens. Zo zorgen wij er voor dat derde partijen jouw persoonsgegevens alleen verwerken voor de afgesproken doelen en onder vooraf vastgestelde voorwaarden.

Verwerking van persoonsgegevens buiten de EU/EER
Persoonsgegevens worden niet door Stichting SKOPOS of haar verwerkers buiten de EU/EER verwerkt. Indien dit het geval is, dan dragen wij er zorg voor dat de persoonsgegevens adequaat worden beschermd.

Wijziging van deze privacyverklaring
Het kan voorkomen dat wij deze privacyverklaring in de toekomst wijzigen. Op onze website: (https://www.skoposschijndel.nl) vind je steeds de actuele verklaring.

Schijndel, 1 maart 2023
Stichting SKOPOS

Bijlage 2: Schema Rollen en Verantwoordelijkheden

De organisatie van IBP gaat over processen, gewoontes, beleid, wetten en regels die van betekenis zijn voor de manier waarop mensen een organisatie sturen, besturen, beheren en controleren. Hierbij spelen de relaties tussen de verschillende betrokkenen en de doelen van de organisatie een rol. Onderstaand overzicht geeft aan welke verantwoordelijkheden en bij welke rollen horen bij Stichting SKOPOS.

Richtinggevend	**Eindverantwoordelijk**	
	Directeur-bestuurder	*Eindverantwoordelijk* *IBP-beleidsvorming, -vastlegging en communiceren ervan* *Verantwoordelijk voor het zorgvuldig en rechtmatig verwerken van persoonsgegevens* *Organisatie IBP inrichten; toewijzen van de taken en rollen* *Evalueren toepassing en werking IBP-beleid op basis van rapportages*
Sturend	**Uitwerken beleid/ inhoudelijk verantwoordelijk**	
	Privacyteam	*Voorbereiden opstellen IBP-beleid, Classificatie/risicoanalyse* *Inhoudelijk verantwoordelijk voor uitwerking van het IBP-beleid* *Adviseert verwerkingsverantwoordelijke (bestuur/CvB/directie) over IBP* *Uitwerken algemeen IBP-beleid naar specifiek beleid op een uniforme manier* *Schrijven en beheren van processen, richtlijnen en procedures om de uitvoering van het IBP-beleid te ondersteunen* *Evalueren van het IBP-beleid en de maatregelen*
	Functionaris voor gegevensbescherming vanuit de Lumengroup ·	*Toezicht houden op naleving privacywetgeving* *Richtlijnen, kaders vaststellen en aanbevelingen doen t.b.v. verbeterde bescherming van verwerkingen van persoonsgegevens* *Voorlichting privacy geven en stimuleren van bewustwording* *Begeleiding, advies en ondersteuning bieden bij de (beveiligings)incidenten* *Kan onafhankelijk optreden als 'ombudsman' bij Afwikkeling IBP-klachten en incidenten.*
	Bovenschools ICT-coördinator	*Risicoanalyse in samenwerking met inhoudelijk verantwoordelijke* *Toegangsbeleid zowel fysieke toegang als digitale toegang vaststellen en laten goedkeuren door de verwerkingsverantwoordelijke* *Regelmatig de (netwerk)toegangsrechten van gebruikers beoordelen, controleren en vastleggen.*
Uitvoerend	**Uitvoeren beleid/ naleven beleid**	
	Privacyteam	*Incidentafhandeling (registreren en evalueren).* *Technisch aanspreekpunt voor IBP-incidenten.* *Uitvoeren taken conform gegeven richtlijnen en procedures.*
	Alle medewerkers	*Verantwoordelijk omgaan met IBP bij hun dagelijkse werkzaamheden.*

	Toezicht naleving en communicatie	
	FG Privacyteam Dagelijkse leiding, directie	*Communicatie naar alle betrokkenen; ervoor zorgen dat medewerkers op de hoogte zijn van het IBP-beleid en de consequenties ervan.* *Toezien op de naleving van het IBP-beleid en de daarbij behorende processen, richtlijnen en procedures door de medewerkers.* *Voorbeeldfunctie met positieve en actieve houding t.a.v. IBP-beleid.* *Implementeren IBP-maatregelen.* *Periodiek het onderwerp informatiebeveiliging onder de aandacht te brengen in werkoverleggen, beoordelingen etc.;*
	Opmerking: *in een aantal gevallen is ook de (G)MR hierbij betrokken.*	

.

Bijlage 3: Functiebeschrijving FG en privacycoördinator

Inleiding
Stichting SKOPOS heeft een externe FG vanuit de Lumen Group. Binnen de Stichting is een privacycoördinator werkzaam die onderdeel uitmaakt van het privacyteam. Zowel voor de FG als voor de privacycoördinator is een functiebeschrijving beschikbaar.

Functionaris Gegevensbescherming
Stichting SKOPOS heeft besloten de functie van Functionaris Gegevensbescherming (hierna: FG) uit te besteden aan de Lumen Group. Gedurende de looptijd van het abonnement is bijgaande regeling met taken en bevoegdheden, die gebaseerd zijn op artikelen 37-39 uit de Algemene Verordening Gegevensbescherming (hierna: AVG), van toepassing. De AVG vereist dat een natuurlijk persoon de functie van Functionaris Gegevensbescherming vervult. Binnen de Lumen Group zal de heer Stijn Sarneel deze functie van FG op zich nemen voor Stichting SKOPOS. Bij de Autoriteit Persoonsgegevens zijn Stijn Sarneel en de Lumen Group voor Stichting SKOPOS reeds aangemeld als zijnde FG.

De FG is een onafhankelijke deskundige op het gebied van gegevensbescherming die als taak heeft om Stichting SKOPOS te adviseren, informeren en om toezicht te houden op de naleving van de AVG. Ook is de FG het aanspreekpunt van de Autoriteit Persoonsgegevens. De vereisten en voorwaarden om een FG aan te stellen zijn wettelijk bepaald in de AVG en dus niet vrijblijvend.
Stichting SKOPOS heeft voor een Lumen Group FG Abonnement gekozen en kiest hiermee voor de volgende diensten:

- Aanstelling van Lumen Group als uw FG inclusief melding en registratie hiervan bij de Autoriteit Persoonsgegevens. Tevens contactpersoon richting Autoriteit Persoonsgegevens indien afstemming of samenwerking nodig is met de toezichthouder.
- Risico-gebaseerde monitoring en toezicht op naleving van de AVG als ‘critical friend'. Wij doen dit door o.a. het verrichten van een AVG-Steekproef en het beoordelen van documenten en werkwijzen. Dit richt zich onder meer op: beleid, getroffen technische- en organisatorische maatregelen, bewustwording personeel en interne audits verband houdende met de bescherming van persoonsgegevens.
- Eén keer per jaar een FG-monitoringsgesprek en één keer per jaar een AVG-Steekproef. Met als resultaat twee keer per jaar een onafhankelijke rapportage van de FG met eventuele bevindingen en aanbevelingen. De rapportage wordt op locatie besproken met hoogste management (inclusief jaarlijkse evaluatie van onze dienstverlening).
- Bereikbaarheid 24/7 voor melding datalekken en begeleiding bij vervolgstappen via het
- Lumen Group Datalek Loket.
- Aanreiken van passende en beproefde AVG-templates en AVG Zelftoets.
- Bereikbaarheid voor en begeleiding bij individuele AVG-vragen en klachten door betrokkenen van uw organisatie (bv. uw personeel en/of uw klanten).
- Begeleiding voorafgaand aan de uitvoering van een Data Protection Impact Assessments (DPIA) en toezicht op correcte (wettelijke) uitvoering hiervan.
- Pushberichten in spoedeisende gevallen (zoals o.a. datalekken bij veelgebruikte leveranciers) en informatie wat dit voor uw organisatie betekent.
- Bereikbaarheid via de Lumen Group Helpdesk voor de eigen privacy coördinator voor eenvoudige vragen die gerelateerd zijn aan de FG (toezichts)functie en de diensten binnen dit abonnement. Mede in het kader van kwaliteitswaarborging beschikt uw organisatie naast een FG ook over een toegewijde en gecertificeerde Privacy Consultant van Lumen Group voor o.a. eerstelijnsvragen.
- Ondersteuning bieden bij het maken van een keuze voor AVG-Tooling of Privacy Management Software en andere AVG/Privacy-producten en -diensten. Wij zijn vertrouwd met deze producten en diensten. Tevens kunnen wij ook deze producten en diensten gebruiken voor de FG (toezichts-)functie (bijv. inlog op afstand) waardoor effectief toezicht houden mogelijk is.

Privacycoördinator
De interne privacycoördinator is s**chakelpunt voor de externe FG van Lumen Group** (bijvoorbeeld bij datalekken, vragen of incidenten). De werkzaamheden en verantwoordelijkheden van een privacycoördinator zijn:

- Coördineren van privacy activiteiten en betrekken medewerkers hierbij.
- Eerste aanspreekpunt voor medewerkers voor vragen of opmerkingen en (potentiële) datalekken.

- Adviseert in samenspraak met de FG van Lumen Group verwerkingsverantwoordelijke (bestuur/CvB/directie) over IBP.
- Voorbereiden, opstellen en beheren IBP-beleid en van onderliggende processen, richtlijnen en procedures die het IBP-beleid ondersteunen.
- Uitwerken algemeen IBP-beleid naar specifiek beleid op een uniforme manier. Schrijven en beheren van processen, richtlijnen en procedures om de uitvoering van het IBP-beleid te ondersteunen.
- Organiseren en verrichten van benodigde risicoanalyses en DPIA's en totstandkoming
- Van een AVG-planning.
- De interne afhandeling van informatieverzoeken, recht van correctie en andere rechten van betrokkenen (zie artikel 12-22 van de AVG).
- Implementeren van privacy- en informatiebeveiligingsmaatregelen samen met andere
- Collega's (multidisciplinair) en bewaken voortgang. Evalueren van het IBP-beleid en de maatregelen.

Bijlage 4: Protocol ICT en Social media voor leerlingen

Algemeen
We behandelen elkaar met respect en laten iedereen in zijn waarde.
Iedereen is verantwoordelijk voor wat hij/zij zelf plaatst op sociale media en kan daarop aangesproken worden.
We helpen elkaar goed en verstandig met internet en sociale media om te gaan en we spreken elkaar daar ook op aan.
Denk altijd na voordat je iets verstuurt.

Je eigen apparaten

1. Onder schooltijd staat je mobiel uit.
2. Je mag met je mobiele telefoon of een ander device geen foto's of filmpjes van de school, een online les, de juf of meester of je medeleerlingen maken en/of doorsturen naar anderen en/of posten op social media of internet.

Internet en e-mail
We vinden het van groot belang dat je als leerling zo veilig mogelijk online kan werken. Om hiervoor te zorgen, zijn de volgende gedragsregels van belang:
Ik gebruik het internet om informatie te zoeken over een onderwerp of werkstuk voor school.
Ik bezoek geen sites die pornografisch, racistisch, discriminerend, beledigend of aanstootgevend zijn.
Ik vraag toestemming van mijn juf of meester, als ik…
Een online game wil spelen.
Persoonlijke gegevens (naam, adres en je telefoonnummer) moet invullen op een website.
Bestanden wil downloaden of delen.
Een e-mail wil versturen.
Mijn mobiele telefoon wil gebruiken
Wees zuinig met je e-mailadres. Je e-mailadres is geld waard! Laat deze dus niet zomaar overal achter.
Ik deel geen wachtwoorden met anderen.
Ik ga voorzichtig om met mails die ik niet vertrouw of waarvan ik de afzender niet ken. Bij twijfel klik ik geen linkjes aan.
Ik vertel direct aan mijn meester of juf als ik informatie tegenkom die ik niet prettig vind of waarvan ik weet dat dat niet hoort.
Ik weet bij welke instanties/personen ik op school en buiten school terecht kan als ik iets onprettigs heb meegemaakt op het internet waarbij ik me niet veilig voel.
Ik bekijk informatie op internet kritisch en kan beoordelen of het echt of nep is.
Als er problemen zijn met een device waarop of het programma waarin je werkt, dan meld ik dit bij mijn juf of meester.
Ik mag alleen met je eigen naam en schoolaccount werken in de programma's die voor jou klaarstaan.
Ik mag zelf geen programma's of apps installeren op de schoolcomputers.
Op vragen om te 'downloaden' is het antwoord altijd 'nee'. Bij twijfel vraag je het aan je meester of juf.
Wanneer je even wegloopt van je plaats achter de computer, vergrendel je je scherm (windowstoets+L).
Als ik klaar ben op de computer log ik uit en sluit ik de computer netjes af.
Buiten de schooltijden mag je de schoolcomputers alleen gebruiken als de juf of meester daar toestemming voor geeft.
Ik ken de gevolgen van het delen van informatie die niet echt is.

Je wachtwoord
De juf of meester legt je uit hoe je een goed wachtwoord bedenkt.
Je mag jouw wachtwoord NOOIT aan een ander geven.
Zorg dat anderen niet kunnen meekijken als je je wachtwoord intypt.
Verander alleen je wachtwoord als de juf of meester daarom vraagt en doe dit dan meteen.
Als je denkt dat een ander jouw wachtwoord kent of gebruikt, vertel dat dan meteen aan je juf of meester.

Sociale media
Binnen de school gelden de volgende gedragsregels om te zorgen dat de mogelijkheden van sociale media worden gebruikt zonder andere personen of de school te schaden:
Ik plaats geen foto's of verhalen over een ander (leerling, juf of meester, school, ouders of anderen van buiten de school) op sociale media als een ander dit niet goed vindt;

Ik plaats geen kwetsende foto's, verhalen of opmerkingen op sociale media. Ook gebruik ik geen grove taal;
Ik doe niet mee aan pesten via social media. Als ik nare berichten ontvang van iemand, dan vertel ik dit op school of thuis;
Als ik iemand niet begrijp op social media, dan vraag ik dit rechtstreeks aan diegene;
Ik ga zorgvuldig om met mijn eigen identiteit. Ik besef dat ik altijd terug te vinden ben op internet.

ICT-apparatuur
De ICT-apparatuur op school (laptop, tablet, 3d-printer, digibord, scanner, etc.) is niet goedkoop, daarom dien je hier voorzichtig mee om te gaan. De volgende gedragsregels zijn daarom van belang:
Ik gebruik alleen ICT-apparatuur en software waar ik toestemming voor heb gekregen van de meester of juf. Dat geldt ook voor meegebracht smartphones, etc.;
Ik ga voorzichtig om met de dure ICT-apparatuur van de school die ik mag gebruiken;
Ik gebruik geen meegebrachte USB-sticks van thuis in ICT-apparatuur van de school en koppel ook geen telefoon een schoolcomputer.

Schermtijd
Ik ben me bewust van de wereld buiten de onlinewereld en ik houd de tijd in de gaten als ik achter de computer/ laptop of tablet zit.

Bijlage 5: Handreiking AVG medewerkers

Hoe bewaar ik bestanden?

Memorysticks raden we af omdat ze snel kwijt kunnen raken. Gebruik voor privacygevoelig materiaal een schijf of cloudservice die beveiligd is met een wachtwoord.

Kan iemand meekijken?

Als er privacygevoelig materiaal op je computer staat, sluit dan altijd je account af, ook wanneer je 'even' wegloopt.

Ben ik de enige die in mijn account kan?

Gebruik alleen je eigen account, dan weet je zeker dat je niet meer ziet dan nodig is voor jouw werkzaamheden. Let ook op dat leerlingen je wachtwoord niet kennen. Surf bewust en controleer of een website een groen slotje heeft.

Is mijn wachtwoord sterk genoeg?

Bedenk een lang, sterk wachtwoord met kleine letters, hoofdletters, cijfers en liefst een die je niet ook ergens anders voor gebruikt. Naam123 en geboortedata vermijden!

Heb ik toestemming?

Weet waar gegevens van leerlingen voor gebruikt mogen worden en met wie je die wel en niet mag delen. Lijstjes met adressen op het prikbord, dat mag niet meer.

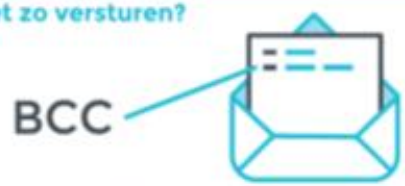
Wat doen we met sociale media?

Spreek af met collega's, ouders en leerlingen wat je plaatst, waar en waarom. Bespreek educatieve en sociale waarden.

Mag ik die foto of video delen?

Bedenk bij iedere foto/video waar leerlingen op voorkomen of er een bezwaar zou kunnen ontstaan als je deze deelt. Jonger dan 16 jaar moeten de ouders toestemming geven. Bij twijfel, raadpleeg de betrokkenen en/of collega's. Deel zo mogelijk via kanalen die aan de AVG voldoen.

Kan ik het zo versturen?



Check of je e-mails BCC verstuurt en dat je alleen privacy-gevoelige informatie deelt via veilige kanalen. Bespreek dit in het team en maak elkaar hiervan bewust. Deel bestanden via AVG-veilige onlinepakketten, liever niet per email.

Is het veilig opgeborgen?

Sluit archiefkasten of ruimtes waar privacygevoelige informatie ligt. Op het kopieerapparaat of in de printerlade blijven soms documenten liggen. Voorkom dat en pak het direct. Vind je zulke informatie? Ga er integer mee om.

Wie is de FG?

Weet wie is aangesteld als Functionaris Gegevensbescherming en meld datalekken zodat hij/zij ze binnen 72 uur bij de Autoriteit Persoonsgegevens kan melden.

Bijlage 6: Protocol beveiligingsincidenten en datalekken

Inleiding
Het Protocol informatiebeveiligingsincidenten en datalekken sluit aan bij de uitgangspunten in het IBP-beleid van Stichting SKOPOS.
Dit protocol biedt een handleiding voor de professionele melding, beoordeling en afhandeling van beveiligingsincidenten en datalekken.

Dit protocol is van toepassing op de gehele organisatie van Stichting SKOPOS en al haar medewerkers.
Gebruikte termen:

- Beveiligingsincident; een beveiligingsincident is een gebeurtenis die ervoor zorgt of zou kunnen zorgen dat de beschikbaarheid, integriteit en/of vertrouwelijkheid van de informatievoorziening wordt aangetast.
- Informatievoorziening; het geheel van mensen, middelen en maatregelen, gericht op de informatiebehoefte van de organisatie.
- Datalek; een beveiligingsincident waarbij persoonsgegevens verloren raken of onrechtmatig worden bewerkt (opgeslagen, aangepast, verzonden, et cetera). Alle datalekken zijn beveiligingsincidenten, maar niet alle beveiligingsincidenten zijn datalekken.
- Betrokkene; de persoon van wie de persoonsgegevens zijn gelekt.

Wet- en regelgeving datalekken
Op 1 januari 2016 is de Wet meldplicht datalekken ingevoerd. Door deze meldplicht zijn ook scholen 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. Als de school gebruik maakt van leveranciers, zoals uitgevers of distributeurs, die persoonsgegevens ontvangen van de school, dan moet de school met deze verwerkers aanvullende afspraken maken over het melden van datalekken.
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’. Dit kan zijn een hack, het verliezen van een usb-stick of de diefstal van een laptop. Maar ook een verkeerd verzonden email of een verkeerd ingestelde autorisatie.
De meldplicht geldt voor de verantwoordelijke voor de persoonsgegevens, dat is dus Stichting SKOPOS. Als er een datalek is, moet **binnen 72 uur** na ontdekking melding worden gedaan bij de Autoriteit Persoonsgegevens.

Afspraken met scholen en leveranciers
Stichting SKOPOS maakt als verantwoordelijke voor de persoonsgegevens de onderstaande datalek-afspraken met de scholen en de leveranciers die persoonsgegevens ontvangen en verwerken:

- De ontdekker van een datalek meldt dit binnen 24 uur bij de directeur van de school of de zaakgelastigde of contactpersoon van een leverancier.
- De directeur of de zaakgelastigde of contactpersoon meldt binnen 24 uur het datalek bij de Functionaris Gegevensbescherming, bij voorkeur fg@lumengroup.nl
- De privacycoördinator neemt de melding op in het Register Datalekken en doet, na een positieve weging, de melding bij de Autoriteit Persoonsgegevens. Ook informeert hij de bestuurder bij een ernstig datalek.

Stichting SKOPOS heeft schriftelijke afspraken met verwerkers over datalekken gemaakt d.m.v. het model verwerkersovereenkomst die hoort bij het convenant “Digitale onderwijsmiddelen en privacy” (www.privacyconvenant.nl).

Werkwijze
De vier rollen
Er zijn tenminste vier rollen die onderscheiden moeten worden om een beveiligingsincident en/of datalek succesvol af te handelen:

1. Ontdekker (medewerker of leerling); degene die het beveiligingsincident of datalek op het spoor komt.
2. Meldpunt (directeur); een aanspreekpunt per school waar alle beveiligingsincidenten worden gemeld.

3. Melder (functionaris gegevensbescherming); degene die verantwoordelijk is voor het melden van een datalek bij de Autoriteit Persoonsgegevens en een incidentenregister bijhoudt.
4. Technicus/ Bovenschools ICT-coördinator; degene die de oorzaak van het datalek kan vinden en kan (laten) repareren.

De 7 stappen

1. Ontdekken

De ontdekker merkt een beveiligingsincident op. Via eigen waarneming of via waarneming van een derde. De ontdekker verzamelt zoveel mogelijk informatie over het beveiligingsincident en meldt dit bij de eigen directeur van de school of de zaakgelastigde of contactpersoon van een leverancier van de school.

2. Inventariseren

De directeur zal samen met de melder de vragenlijst in de bijlage zo compleet mogelijk invullen.

3. Beoordelen

Wanneer de vragenlijst is ingevuld, stuurt de directeur - nog op dezelfde dag van de ontdekking- het formulier naar de privacycoördinator – privacy@skoposschijndel.nl - met het verzoek het datalek te beoordelen.

De privacycoördinator informeert na ontvangst van het meldingsformulier direct de directeur-bestuurder en FG.

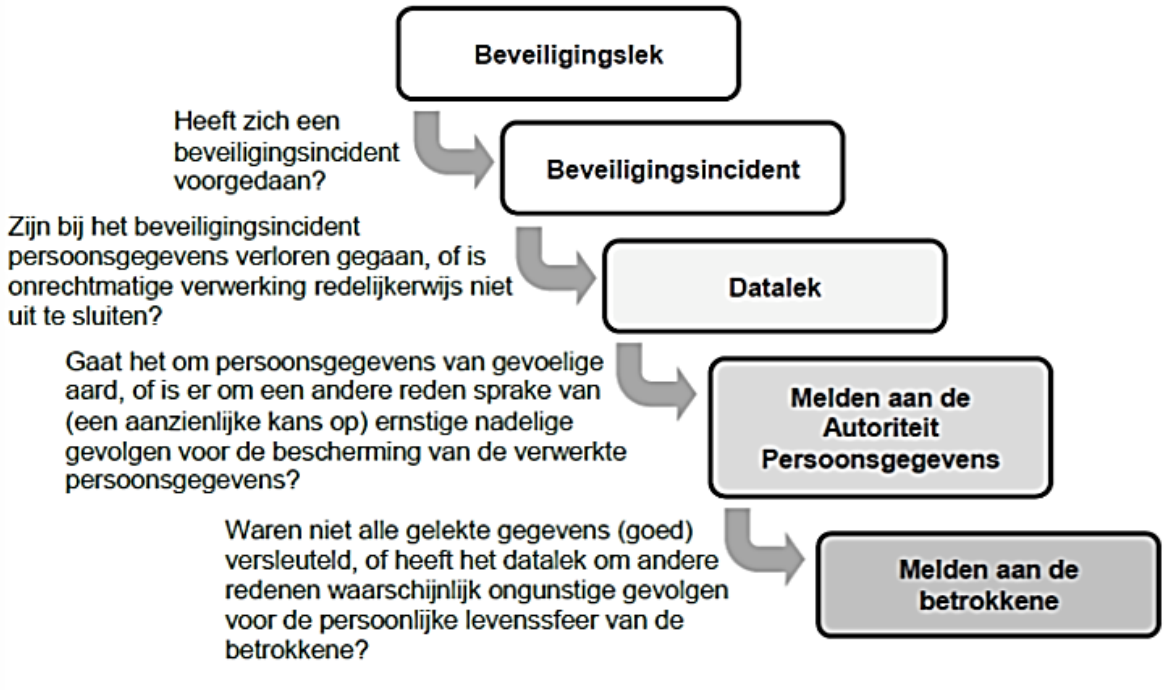
De FG beoordeelt de informatie om te bepalen of ook een melding aan de Autoriteit persoonsgegevens vereist is en informeert de directeur-bestuurder en privacycoördinator over zijn conclusie.

De volgende informatie over het datalek wordt vastgelegd door de privacycoördinator:

- De feiten rondom het datalek en de mogelijke gevolgen van het datalek het ingevulde meldingsformulier.
- Is het datalek gemeld aan de Autoriteit Persoonsgegevens? Waarom niet?
- De inhoud van de melding.
- Is het datalek gemeld aan de betrokkenen? Waarom niet?

Bij de beoordeling of er sprake is van een ‘meldingsplichtig datalek’, houdt de FG rekening met het type gegevens, en met de hoeveelheid gegevens. Indien het datalek een risico inhoudt voor de rechten en vrijheden van de betrokkenen wordt er gemeld bij de Autoriteit Persoonsgegevens.

De onderstaande beslisboom wordt gebruikt:



4. Beperken gevolgen
De gevolgen worden zoveel mogelijk beperkt. Er wordt gekeken wat de oorzaak van het beveiligingsincident is. De nodige acties voor de aanpak en het verhelpen van de oorzaak worden uitgevoerd.

5. Melden
Indien de conclusie bij stap 3 is dat er melding gedaan moet worden bij de Autoriteit Persoonsgegevens, dan zal de privacycoördinator dit binnen een werkdag doen. De melding bevat alle verzamelde informatie en de getroffen incidentele en structurele technische en organisatorische maatregelen. Het lek wordt gemeld bij het meldloket datalekken: https://datalekken.autoriteitpersoonsgegevens.nl/actionpage?0.

6. Vastleggen
Alle informatie, die in de voorafgaande stappen is ingewonnen of ontstaan, wordt gearchiveerd door de privacycoördinator waarmee het incident is afgesloten. De privacycoördinator informeert de directeur van de school over de genomen (te nemen) maatregelen om herhaling te voorkomen.

7. Informeren betrokkene: leerling en/of zijn ouders
Wanneer het datalek waarschijnlijk een hoog risico inhoudt voor de betrokkene(n), dan wordt het datalek ook aan de betrokkene(n) zelf gemeld. Dat zijn medewerkers, leerlingen, of hun ouders als zij jonger zijn dan 16 jaar.

In principe wordt ervan uitgegaan dat het lekken van persoonsgegevens van (minderjarige) leerlingen altijd van gevoelige aard is en gemeld moet worden bij de betrokkenen.
Als er persoonsgegevens zijn gelekt maar die zijn beveiligd of versleuteld, en de gelekte data zijn volledig onbegrijpelijk of ontoegankelijk voor anderen, dan hoeft dat niet aan betrokkenen te worden gemeld.

Monitoring beveiligingsincidenten en datalekken
De FG maakt jaarlijks een analyse van de meldingen van de beveiligingsincidenten en de datalekken.
In de analyse wordt ingegaan op eventuele structurele ontwikkelingen, en of de noodzaak bestaat om maatregelen te nemen om herhaling te voorkomen.
De directeur-bestuurder wordt door de FG geïnformeerd over de uitkomsten van de analyse.

Meldingsformulier beveiligingsincident/ datalek (invullen en insturen door directeur)

Dit formulier invullen en insturen door directeur van de school naar: privacy@skoposschijndel.nl

- Beveiligingsincident; een beveiligingsincident is een gebeurtenis die ervoor zorgt of zou kunnen zorgen dat de beschikbaarheid, integriteit en/of vertrouwelijkheid van de informatievoorziening wordt aangetast.
- Datalek; een beveiligingsincident waarbij persoonsgegevens verloren raken of onrechtmatig worden bewerkt (opgeslagen, aangepast, verzonden, et cetera). Alle datalekken zijn beveiligingsincidenten, maar niet alle beveiligingsincidenten zijn datalekken.

1 Datum/periode van het beveiligingsincident / datalek.

2 Gegevens van de melder (naam, functie, hoe te bereiken).

3 Gegevens school.

Naam school : _____

Naam, e-mail en telefoonnummer directeur : _____

4 Toedracht van het incident.

5 Korte beschrijving van het incident (bijv. verlies, diefstal).

6 Wat voor soort gegevens zijn er bij het incident betrokken (welke persoonsgegevens)?

7 Wie is er verantwoordelijk voor het datalek (welke persoon of organisatie)?

8 Welke actie is al ondernomen?

Bijlage 7: Jaarlijks Toestemmingsformulier gebruik beeldmateriaal

Beste ouder/verzorger,

Op onze school laten wij u met beeldmateriaal zien waar we mee bezig zijn. Opnames worden gemaakt tijdens verschillende gelegenheden. Bijvoorbeeld tijdens activiteiten, schoolreisjes en lessen. Ook uw zoon/dochter kan op deze foto's (en soms in video's) te zien zijn.
Natuurlijk gaan we zorgvuldig om met het beeldmateriaal. We plaatsen bij het beeldmateriaal geen namen van leerlingen.

Met dit formulier vragen we uw toestemming voor het gebruik van beeldmateriaal van uw zoon/dochter. Wilt uw de antwoordstrook met uw kind meegeven en afgeven aan de leerkracht? Per kind een apart formulier invullen a.u.b.

Deze toestemming geldt alleen voor foto's en video's die door ons, of in onze opdracht worden gemaakt. Het kan voorkomen dat andere ouders foto's maken tijdens schoolactiviteiten. De school heeft daar geen invloed op en is daar niet voor verantwoordelijk.
Daarnaast vragen wij uw toestemming voor het delen van de klassenfoto met klasgenoten.
Wilt u uw toestemming samen met uw zoon/dochter bespreken? We merken dat oudere leerlingen soms zelf een keuze willen maken om foto's te gebruiken. Als u uw keuze thuis bespreekt, dan weten ze zelf waarom het gebruik van beeldmateriaal wel of niet mag.
Als we beeldmateriaal voor een ander doel willen gebruiken, vragen we u apart om toestemming.
U mag natuurlijk altijd uw toestemming weer intrekken. Geef dit dan door aan de directeur.
Alvast bedankt voor uw medewerking!

Met vriendelijke groet,
[Naam directeur]

✂----------

Hierbij geeft ondergetekende, ouder/ verzorger van …… Groep …….

1. **Wel** / **Geen*** toestemming dat …… *[NAAM school]* …… klassenfoto's maakt die met klasgenoten gedeeld worden
   (*doorhalen wat NIET van toepassing is)
2. Toestemming voor gebruik beeldmateriaal**
   (**hieronder aankruisen waarvoor u toestemming geeft)

☐ in de schoolgids	☐ op de website van school
☐ in oudercommunicatietool (app/website)	☐ op sociale media
☐ in nieuwsbrieven	☐ in persberichten door school aangeleverd

Datum : ----------

Naam ouder(s) / verzorger(s) : ----------

Handtekening ouder(s) / verzorger(s) : ----------

Bijlage 8: Eenmalige toestemming adresgegevens, tel.nr. en e-mailadres

Beste ouder/verzorger,

Met dit formulier vragen we uw toestemming voor het gebruik van adres, telefoon en e-mailadres van uw zoon/dochter. Wij verzoeken u onderstaande gegevens in te vullen en in te leveren bij de directeur van de school.

Met vriendelijke groet,
…… *[NAAM school]*……

…… *[NAAM Directeur]* ……

Eenmalige toestemming adres, telefoon en e-mailadres:

Hierbij verklaart ondergetekende, ouder / verzorger van:

Naam leerling : ---------- Groep : ----------

Naam leerling : ---------- Groep : ----------

Naam leerling : ---------- Groep : ----------

Naam leerling : ---------- Groep : ----------

	JA	NEE
Dat de adreslijst met de naam van mijn kind, adres en telefoonnummer verspreid mag worden in de klas van mijn kind *	☐	☐
Dat het e-mailadres van de ouder/verzorger verspreid mag worden in de klas van mijn kind *	☐	☐
Dat de adreslijst, het telefoonnummer en e-mailadres gebruikt mogen worden voor het verstrekken van school specifieke informatie en onderwijsdoeleinden *	☐	☐

(* *a.u.b. aankruisen waarvoor u toestemming geeft*)

Datum : ----------

Naam ouder(s) / verzorger(s) : ----------

Handtekening ouder(s) / verzorger(s) : ----------

Bijlage 9: Geheimhoudingsverklaring

Beleid en maatregelen zijn niet voldoende om persoonsgegevens passend te beschermen. De feitelijke omgang met persoonsgegevens door alle medewerkers die werkzaam zijn voor Stichting SKOPOS dient zorgvuldig te zijn en in overeenstemming met de AVG. Dat betekent dat al deze personen de persoonsgegevens die zij verwerken, geheim dienen te houden. Dit wordt geregeld d.m.v. deze geheimhoudingsverklaring.

Ondergetekende:

Naam	:	.....
Rol / functie binnen Stichting SKOPOS	:	.....
Organisatieonderdeel/ school	:	_____

Hierna te noemen: werknemer

Overwegende:

dat werknemer een dienstverband in het kader van de CAO PO heeft bij Stichting SKOPOS.

dat werknemer voor de uitvoering van zijn of haar functie de beschikking moet hebben over informatie en/of persoonsgegevens, door Stichting SKOPOS verzameld in haar hoedanigheid als verantwoordelijke in de zin van de algemene verordening gegevensbescherming.

dat Stichting SKOPOS wil benadrukken dat zij de zorgvuldige omgang met deze gegevens van groot belang vindt en daarom voorwaarden stelt aan het ter beschikking stellen van deze gegevens aan werknemer.

dat Stichting SKOPOS tevens moet voldoen aan haar wettelijke verplichting tot het treffen van technische en organisatorische beveiligingsmaatregelen ten aanzien van deze informatie en/of persoonsgegevens.

dat werknemer door het ondertekenen van deze verklaring erkent dat Stichting SKOPOS deze informatie en/of persoonsgegevens als geheim en vertrouwelijk beschouwt en dat werknemer schade kan berokkenen door onzorgvuldige omgang met en/of het onrechtmatig aan derden ter beschikking stellen van deze informatie.

Verklaart dat:

de werknemer de informatie en/of persoonsgegevens alleen zal gebruiken voor de duur van het dienstverband en uitsluitend voor de werkzaamheden binnen de functie van de werknemer.

de werknemer de informatie en/of persoonsgegevens niet zonder voorafgaande toestemming van Stichting SKOPOS verstrekt aan derden.

de werknemer uiterste zorg besteedt aan een deugdelijke en veilige opslag van de informatie en/of persoonsgegevens, ter voorkoming van verlies en/of enige vorm van onrechtmatige verwerking, en hiertoe de richtlijnen en instructies opvolgt die Stichting SKOPOS verstrekt en voorschrijft.

het voorgaande geldt ook voor, door of namens stichting SKOPOS verstrekte toegang aan werknemer tot ICT-systemen en/of ter beschikking gestelde apparatuur.

de werknemer zich verplicht alle door of Stichting SKOPOS verstrekte informatie en/of persoonsgegevens te retourneren aan Stichting SKOPOS, zodra daarom verzocht wordt. De werknemer zal geen kopieën van de informatie bewaren.

de werknemer erkent dat Stichting SKOPOS altijd rechthebbende en eigenaar blijft van de verstrekte informatie en/of persoonsgegevens.

de afspraken in deze verklaring ook na beëindiging van het dienstverband geldig blijven.

Ondertekening:

plaats	:	.....
datum	:	.....
naam	:	.....
handtekening	:	_____

Bijlage 10: IBP bij leerlingdossiers en onderwijskundige rapporten (zoals bij OSO en LDOS)

Leerlingdossiers

- U mag alleen gegevens verwerken in het leerlingdossier voor zover dat noodzakelijk is voor het doel.
- De gegevens die u verwerkt in het leerlingdossier, moeten juist zijn.
- U regelt de beveiliging van en de toegang tot de leerlingdossiers goed.
- U kunt aantonen dat u bij het gebruik van leerlingdossiers de regels van de AVG naleeft. Dit heet de verantwoordingsplicht.
- U neemt de gegevensverwerking in leerlingdossiers op in uw register van verwerkingsactiviteiten.
- U kunt verplicht zijn om een data protection impact assessment (DPIA) uit te voeren voor uw gebruik van het leerlingdossier.
- Houd er rekening mee dat ouders en/of leerlingen het recht op dataportabiliteit hebben. Dat is het recht om gegevens mee te nemen. Bijvoorbeeld naar een andere school.

Onderwijskundig rapport

- Een basisschool mag alleen gegevens over een leerling in het onderwijskundig rapport opnemen die in de volgende categorieën vallen volgens het Besluit uitwisseling leer- en begeleidingsgegevens:
- Administratieve gegevens (zoals naam, adres en onderwijsnummer van de leerling);
- Gegevens over onderwijshistorie en leerresultaten (zoals een eventuele overstap tussen scholen en toetsresultaten);
- Gegevens over de sociaal-emotionele ontwikkeling en het gedrag van het kind (zoals het gedrag in de omgang en zijn/haar werkhouding);
- Gegevens over de eventuele extra begeleiding die het kind heeft gekregen of nodig heeft;
- Gegevens over de verzuimhistorie (ongeoorloofd verzuim van het kind in het jaar voorafgaand aan het onderwijskundig rapport).
- Het onderwijskundig rapport wordt bewaard tot vijf jaar na uitschrijving van de leerling.

Bijlage 11: Overzicht bewaartermijnen

Bewaartermijn leerlinggegevens

- In het lager en voortgezet onderwijs geldt dat u gegevens over verzuim en afwezigheid en in- en uitschrijving 5 jaar moet bewaren nadat de leerling is uitgeschreven.
- Gegevens over een leerling die naar een school voor speciaal onderwijs is doorverwezen, moet u als school 5 jaar na het vertrek van de leerling bewaren.
- Een school mag adresgegevens van oud-leerlingen bewaren voor het organiseren van reünies. Let er wel op dat hiervoor eerst toestemming gevraagd wordt aan de oud-leerlingen. Deze gegevens mogen alleen voor dat doel gebruikt worden.

Bewaartermijn personeelsgegevens

Hoe lang mag een Stichting het personeelsdossier bewaren?
De bewaartermijnen van personeelsgegevens zijn afhankelijk van verschillende wetgeving.

Sollicitatiegegevens

Deze informatie (sollicitatiebrief, cv., gespreksaantekeningen) wordt uiterlijk na 4 weken vernietigd tenzij met de sollicitant anders is overeengekomen. Een assessment of psychologisch onderzoek kan deel uitmaken van de procedure. Ook deze gegevens worden uiterlijk na vier weken, nadat de procedure is beëindigd, vernietigd, met uitzondering van de gegevens van degene die in dienst genomen wordt.

Personeelsgegevens

Over het algemeen geldt voor personeelsgegevens een bewaartermijn van twee jaar nadat het dienstverband is beëindigd. Mochten die gegevens echter in een eerdere fase al niet meer nodig zijn, dan moeten ze direct verwijderd worden.
Gegevens van (ex-)werknemers kunnen langer bewaard worden indien er een arbeidsconflict met deze persoon is (geweest) of als er een rechtszaak loopt. Tevens mogen gegevens langer bewaard worden als een (ex-)werknemer hiervoor toestemming heeft gegeven. Geadviseerd wordt om gegevens van ex-medewerkers, die nog moet bewaard worden, van het actieve bestand naar een passief bestand te verplaatsen.
In tegenstelling tot de archiefwet is de belastingwetgeving wel van toepassing. Voor gegevens uit de salarisadministratie die fiscaal van belang zijn, bestaat een bewaarplicht van zeven jaar na het einde van de dienstbetrekking. Daarnaast moeten loonbelastingverklaringen en kopieën van een identiteitsbewijs tot vijf jaar na het einde van de dienstbetrekking bewaard worden.

Vernietiging of archiefbestemming

Als persoonsgegevens niet meer nodig zijn of de bewaartermijn is verlopen, dan moeten die gegevens verwijderd worden. Verwijderen betekent niet dat de gegevens vernietigd moeten worden.

Het is voldoende de gegevens buiten het bereik van de actieve administratie te brengen en in een archief of op een aparte schijf op te slaan.
Stichting SKOPOS mag, op vrijwillige basis, persoonsgegevens in een archief bewaren dat bestemd is voor historische, statistische of wetenschappelijke doeleinden mits hierbij voldaan wordt aan de eisen m.b.t. bescherming van deze gegevens volgens de AVG.
Men moet zorgvuldig met de vernietiging van papieren en digitale gegevens omgaan. De gevoeligheid van persoonsgegevens (leerling of medewerker) is groot. Met het oog hierop is een oud-papierbak niet de juiste plaats om deze gegevens in af te voeren. Een papierversnipperaar of een in vertrouwelijk papierafvoer gespecialiseerd bedrijf is de aangewezen weg. Voor digitaal opgeslagen gegevens geldt dataminimalisatie en zijn systemen beschikbaar die automatisch gegevens vernietigen op een van tevoren aangegeven tijdstip. De harde schijven van de devices worden ook door een gespecialiseerd bedrijf vernietigd.