Informatiebeveiligings- en privacybeleid (IBP)

Stichting SKOPOS

Versiebeheer

Datum	***Auteur***	***Versie***	***Status***	***Aanpassing***
15-04-2026	Privacyofficer	1	goedgekeurd	----

Naam:	Informatiebeveiligings- en privacybeleid (IBP)
Versie:	1.0 – april 2026
Type:	Beleid
Relatie met norm(en):	GO.02 Beleid informatiebeveiliging BL.01 Privacybeleid
Relatie met andere documentatie:	PR.07 Bewaartermijnenoverzicht SW.02 IBP bij leerlingdossiers en onderwijskundige rapporten GB.01 Beveiligingsincidenten en datalekkenregister HR.06 Geheimhoudingsbepaling HR.06 Handreiking AVG medewerkers PR.03 Verwerkingsregister RB.02 Privacyreglement Leerlingen en ouders RB.02 Privacyreglement Medewerkers RB.02 Privacyverklaring GB.01 Incidentmanagementproces HR.06 Protocol ICT en Social Media Medewerkers HR.06 Protocol ICT en Social Media Leerlingen OI.04 Protocol gebruik beeldmateriaal door medewerkers en ouders OI.01 Reglement Functionaris Gegevensbescherming PH.01 Reglement Cameratoezicht BC.01 Bedrijfscontinuïteitsplan (BCP) OI.04 Bewustwordingsprogramma CO.01 Configuratiemanagementdatabase (CMDB) ID.01 Identiteits- en toegangsbeheer SC.01 Leveranciersmanagementproces BC.03 Procesbeschrijving Back-up en Herstel SM.01 Procesbeschrijving Securitymanagement RM.01 Risicomanagementbeleid SM.01 Securitybaseline
Eindverantwoordelijk:	Directeur Bestuurder Stichting SKOPOS
Eigenaar:	Privacy Officer
Vastgesteld op/door	Datum vaststelling: 09-06-2026 S. Notenboom (directeur bestuurder) M. van Herwijnen (voorzitter GMR)
PDCA-termijn:	3 jaar

Inhoudsopgave

Inhoud

1 Inleiding 4

1.1 Onze intentie 4

1.2 Doelstelling 4

1.3 Reikwijdte 5

2 Juridisch kader 5

2.1 Wettelijke en reglementaire kaders 5

2.2 Normen en standaarden 5

3 Eigenaarschap en verantwoordelijkheden 6

3.1 Drie-lijns-model 6

3.1.1 Eerste lijn: eindverantwoordelijkheid bij het bestuur 6

3.1.2 Tweede lijn: adviseren en ondersteunen 6

3.1.3 Derde lijn: onafhankelijke controle 7

3.2 Medezeggenschap 7

4 Beleidsthema's informatiebeveiliging 7

4.1 Risicomanagement 8

4.2 Kennis en Afhankelijkheid medewerkers 8

4.3 Bedrijfscontinuïteit 8

4.4 Back-up en herstel 9

4.5 Fysieke beveiliging 9

4.6 Systeem- en data-eigenaarschap en configuratiebeheer 9

4.7 Classificatie van systemen en data 10

4.8 Securitybaseline 10

4.9 Bewustwording 11

4.10 Incident- en problemmanagement 11

4.11 Risicomanagement leveranciers 12

4.12 Werkplekken en mobiele apparaten 12

4.13 Identiteits- en toegangsbeheer 12

4.14 Securitymanagement 13

4.14.1 Vulnerabilitymanagement en pentesting 13

4.14.2 Patchmanagement 13

4.14.3 Logging 13

4.14.4 Digitaal sleutelbeheer 13

5 Uitgangspunten privacy 14
Persoonsgegevens 14
Privacyvuistregels 14
6 Beleidsthema's privacy 16
6.1 Verwerkingsregister 16
6.1.1 Legitiem doel en doelbinding 16
6.1.2 Grondslag 17
6.2 Informatieplicht 18
6.3 Toestemming 18
6.4 Privacy by design en privacy by default 18
6.4.1 Dataminimalisatie 19
6.5 Bewaartermijnen 19
6.6 Afhandelen van datalekken 19
6.7 Data Protection Impact Assessment 19
6.8 Uitwisseling persoonsgegevens 20
6.8.1 Gegevensverwerking buiten de EER 20
6.9 Rechten van betrokkenen 20
7 Verantwoording IBP 21
7.1 Naleving AVG 21
7.2 Rapportage 21
7.3 Beleidsherziening 21
Bijlage 1 Overzicht vastgestelde documenten 22
Bijlage 2 Lijst met afkortingen 23

1 Inleiding

Het onderwijs is in toenemende mate afhankelijk van informatie en ICT. Lesmateriaal wordt digitaal aangeboden, toetsingsprogramma's worden digitaal en de resultaten en ontwikkelingen van leerlingen worden opgenomen in een digitaal leerlingvolgsysteem. Daarnaast wordt ook veel gebruikgemaakt van digitale communicatie tussen de school, leerlingen en ouders/verzorgers. Door deze ontwikkelingen neemt het risico op verstoring van het onderwijs, verlies of misbruik van gegevens en overmatige dataverzameling toe. Het is de verantwoordelijkheid van Stichting SKOPOS om dat te voorkomen en een veilige leeromgeving te bieden.

Dit beleid voor informatiebeveiliging en privacy (IBP-beleid) beschrijft hoe Stichting SKOPOS omgaat met de beveiliging van informatie en hoe de verwerking van (persoons)gegevens wordt gewaarborgd en gehandhaafd. In het beleid worden de verschillende rollen en verantwoordelijkheden binnen Stichting SKOPOS op het gebied van informatiebeveiliging en privacy (IBP) beschreven.

1.1 Onze intentie

Stichting SKOPOS draagt de verantwoordelijkheid voor het creëren van een veilige werk- en leeromgeving. Dit houdt in dat Stichting SKOPOS passende technische en organisatorische maatregelen toepast om informatie te beschermen en ongeoorloofde toegang, verlies of misbruik te voorkomen.
Het recht op privacy is een grondrecht. Iedereen heeft recht op privacy en bescherming van de persoonlijke levenssfeer. Dit geldt vanzelfsprekend ook voor leerlingen, ouders/verzorgers, medewerkers en docenten. Stichting SKOPOS is verantwoordelijkheid voor het waarborgen van de privacy van de leerlingen en het personeel. Dit betekent ook dat deze betrokkenen zeggenschap hebben over het gebruik van hun persoonsgegevens, zoals wettelijk bepaald.
Bij Stichting SKOPOS staat het bieden van goed onderwijs voorop. Om dit te kunnen doen verwerken wij diverse persoonsgegevens van leerlingen, ouders/verzorgers, medewerkers en docenten. Stichting SKOPOS vindt het belangrijk om informatie goed te beschermen en veilig en verantwoord met persoonsgegevens om te gaan. Het goed regelen van informatiebeveiliging en privacy in een beleid is noodzakelijk om de gevolgen van mogelijke informatiebeveiliging- en privacyrisico's tot een aanvaardbaar niveau terug te brengen en de voortgang van het onderwijs te kunnen waarborgen.

1.2 Doelstelling

Dit IBP-beleid is erop gericht de kwaliteit van de verwerking van (persoons)gegevens en de beveiliging van informatie en systemen te verhogen. Hierbij moet een juiste balans bestaan tussen veiligheid, privacy en functionaliteit. Het uitgangspunt is dat een veilige werk- en leeromgeving wordt gecreëerd, de persoonlijke levenssfeer van de betrokkenen wordt gerespecteerd en Stichting SKOPOS voldoet aan relevante wet- en regelgeving. Dit gebeurt onder andere door bewustwording te vergroten over het belang van het zorgvuldig omgaan met informatie, systemen en persoonsgegevens.
Stichting SKOPOS maakt gebruik van het 'Normenkader Informatiebeveiliging en Privacy voor het onderwijs' – oftewel het Normenkader IBP - om inzichtelijk te maken waar de organisatie nu staat en welke maatregelen genomen moeten worden om een veilige werkomgeving te creëren en te voldoen aan de AVG. In 2029 voldoen we minimaal aan volwassenheidsniveau 3 op alle onderdelen van het normenkader.

1.3 Reikwijdte

Dit beleid is van toepassing op alle leerlingen, docenten, medewerkers, bezoekers, ouders/verzorgers, derde partijen en andere gebruikers die toegang hebben tot of werken met de informatie van Stichting SKOPOS. Het beleid heeft betrekking op de verwerking van alle soorten gegevens en informatie waaronder; persoonsgegevens, bedrijfsinformatie en technische gegevens. Het is van toepassing op alle gegevensverwerkingen die onder de AVG vallen.

Informatiebeveiliging en privacy maken integraal onderdeel uit van dit IBP-beleid. Informatiebeveiliging is een belangrijke voorwaarde voor privacy. Informatiebeveiliging omvat de beveiliging van *alle* informatie, terwijl privacy gaat over de verwerking van persoonsgegevens.

2 Juridisch kader

2.1 Wettelijke en reglementaire kaders

Het juridisch kader voor dit IBP-beleid wordt gevormd door de Algemene Verordening Gegevensbescherming (AVG) en de Uitvoeringswet UAVG. Daarnaast kunnen uit andere wet- en regelgeving verplichtingen of instructies voortvloeien voor de verwerking van persoonsgegevens. Voor Stichting SKOPOS is op dit gebied onder andere de volgende wetgeving van belang:

- Wet op het primair onderwijs en/of Wet voortgezet onderwijs en/of Wet op de expertisecentra
- Wet onderwijstoezicht
- Archiefwet en Archiefbesluit
- Leerplichtwet
- Wet medezeggenschap op scholen
- Arbeidsregelgeving en CAO
- Belastingwetgeving
- Telecommunicatiewet en e-privacy wetgeving
- Europese AI-verordening

Indien een (mogelijke) strijdigheid tussen dit beleid en de AVG en/of gerelateerde wet- en regelgeving bestaat, dan moet voorafgaand aan een verwerking overlegd worden met Functionaris Gegevensbescherming.

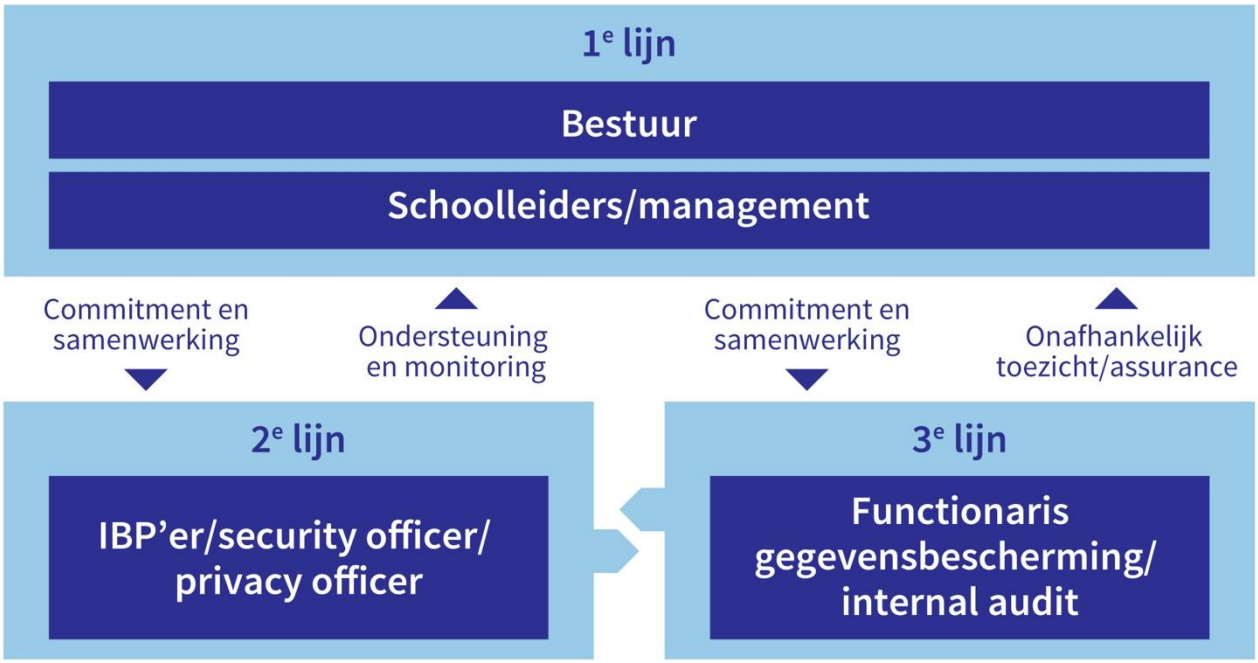
2.2 Normen en standaarden

Als onderwijssector hebben we afgesproken om toe te werken naar één normenkader om aan de minimale vereisten te voldoen voor digitaal veilig onderwijs. Dit is het ‘Normenkader Informatiebeveiliging en Privacy voor het onderwijs’. Dit normenkader beschrijft de regels, principes en standaarden op het gebied van informatiebeveiliging en privacy waaraan Stichting SKOPOS moet voldoen voor een digitale veilige schoolomgeving.

3 Eigenaarschap en verantwoordelijkheden

Dit hoofdstuk beschrijft hoe de verschillende rollen en verantwoordelijkheden met betrekking tot informatiebeveiliging en privacy samenhangen.

3.1 Drie-lijns-model



Informatiebeveiliging en privacy bij Stichting SKOPOS is ingericht volgens het drie-lijns-model (3L-model). Het 3L-model is een leidraad bij het inrichten van de governance van een organisatie.

3.1.1 Eerste lijn: eindverantwoordelijkheid bij het bestuur

Het 3L-model heeft als uitgangspunt dat de eerste lijn verantwoordelijk is voor processen, informatie en systemen van de organisatie, de risico's die hieruit voortvloeien en het treffen van de juiste maatregelen om de risico's te verkleinen. De eerste lijn bestaat uit het bestuur, directeuren, en het verdere lijnmanagement van Stichting SKOPOS
Het bestuur is binnen de eerste lijn eindverantwoordelijk voor informatiebeveiliging en privacy, maar kan bepaalde verantwoordelijkheden beleggen bij andere functies binnen de organisatie. Bij de beschrijving van de beleidsthema's in hoofdstuk 4 en 6 wordt per thema beschreven wie er verantwoordelijk is.

3.1.2 Tweede lijn: adviseren en ondersteunen

Naast de eerste lijn moet er een rol zijn die de eerste lijn ondersteunt, adviseert, coördineert en die bewaakt of het management de verantwoordelijkheden ook daadwerkelijk neemt. Dit is de tweede lijn. De tweede lijn bestaat uit de privacy officer, IBP-adviseurs en juridische adviseurs.

3.1.3 Derde lijn: onafhankelijke controle

De derde lijn controleert of de eerste en tweede lijn soepel samenwerken en goed functioneren. De derde lijn is onafhankelijk, opereert los van de andere organisatieonderdelen en suggereert waar nodig verbeteringen. De functionaris gegevensbescherming (FG) en de accountant vallen binnen de derde lijn. De FG wordt aangesteld door het bestuur en heeft een wettelijk omschreven en onafhankelijke toezichthoudende taak. De FG werkt via een reglement dat door het bestuur wordt vastgesteld.

3.2 Medezeggenschap

Stichting SKOPOS betrekt de gemeenschappelijke medezeggenschapsraad (GMR) bij besluiten over regelingen en procedures ten aanzien van de bescherming van persoonsgegevens. Het bestuur is eindverantwoordelijk voor het informeren van de gemeenschappelijke medezeggenschapsraad en voor het opstellen van instemmingsprocedures.

4 Beleidsthema's informatiebeveiliging

Dit hoofdstuk beschrijft de beleidsthema's op het gebied van informatiebeveiliging.
Een betrouwbare en veilige omgang met informatie is essentieel voor het functioneren van onze organisatie. Informatiebeveiliging en privacybescherming vormen hierbij een continu proces, waarbij we als organisatie streven naar een aantoonbaar volwassen en risicobewust niveau van werken. Het normenkader dient daarbij als ons toetsingsinstrument: het geeft inzicht in waar we staan, waar risico's zich bevinden en welke stappen nodig zijn om onze informatiehuishouding structureel te versterken.

Binnen dit normenkader hanteren we een volwassenheidsmodel van niveau 1 t/m 5. Ons strategisch doel is om in 2029 minimaal volwassenheidsniveau 3 te bereiken. Dat betekent dat processen niet alleen beschreven zijn, maar ook daadwerkelijk worden toegepast en periodiek worden beoordeeld op effectiviteit.

Om dit te realiseren zullen alle relevante onderdelen van informatiebeveiliging en privacy systematisch tegen het licht worden gehouden. Bijbehorende acties, maatregelen en documentatie worden toegevoegd en waar nodig herzien. We hanteren een roadmap die binnen onze GRC-tooling[1] wordt bijgehouden, zodat we gestructureerd toewerken naar het gewenste volwassenheidsniveau.

Deze aanpak waarborgt dat informatiebeveiliging en privacy niet slechts verplichtingen zijn, maar integraal onderdeel worden van onze manier van werken; transparant, beheerst en toekomstbestendig.

Onderstaande items van dit hoofdstuk zijn opgenomen in het groeipad van het normenkader.

[1] Governance, Risk & Compliance is software die helpt om risicobeheer en naleving van wetgeving centraal te beheren, automatiseren en inzichtelijk te maken. We gebruiken hiervoor de tool Your Safety Net (YSN).

4.1 Risicomanagement

Stichting SKOPOS gaat een losstaand Risicomanagementbeleid hanteren.

4.2 Kennis en Afhankelijkheid medewerkers

Stichting SKOPOS is voor de beveiliging van informatie en de continuïteit van het onderwijs afhankelijk van de kennis en beschikbaarheid van medewerkers. Stichting SKOPOS wil voorkomen dat er onvoldoende kennis aanwezig is bij medewerkers of dat kritieke kennis en vaardigheden onvoldoende aanwezig zijn binnen de organisatie. Taken van sleutelfiguren moeten daarom altijd overgenomen kunnen worden door andere medewerkers.

Hiervoor hanteert Stichting SKOPOS de volgende maatregelen:

- Een back-upplan voor kritieke medewerkers.
- Voldoende training en certificering.
- Een indienst-/uitdiensttredingproces waarin rekening gehouden wordt met aansluiting op het proces voor het beheren van rechten en rollen, de overdracht van kennis en documentatie en screening van medewerkers.

Verantwoordelijkheden:

- Bestuur is verantwoordelijk voor het formeel goedkeuren van het back-upplan voor kritieke medewerkers.
- BICT (Bovenschools ICT) is verantwoordelijk voor het opstellen en het beheren van het back-upplan voor kritieke medewerkers.
- HR is verantwoordelijk voor het opstellen en het beheren van het indienst-/ uitdiensttreding proces.

4.3 Bedrijfscontinuïteit

Stichting SKOPOS zorgt ervoor dat mogelijke verstoringen van het onderwijs zo snel mogelijk verholpen worden en dat de impact van verstoringen beperkt blijft. Door processen te analyseren worden de meest kritieke applicaties en medewerkers geïdentificeerd, en wordt bepaald welke terugvalopties nu aanwezig zijn. Hierna kunnen maatregelen geïmplementeerd worden om verstoringen zo veel mogelijk te voorkomen of de impact te beperken. Er is een crisismanagementteam aanwezig om snel en adequaat op incidenten te reageren.

Stichting SKOPOS hanteert de volgende maatregelen voor bedrijfscontinuïteit:

- **Business impact analyses (BIA) op basis van de processen van de organisatie**. De processen worden op basis van een risico gestuurde aanpak geanalyseerd, waarbij eerst de meest kritieke processen behandeld worden. Nieuwe risico's die tijdens deze BIA's geïdentificeerd zijn, worden opgenomen in het risicoregister. Zie hiervoor het risicomanagementbeleid.
- **Een bedrijfscontinuïteitsplan (BCP)**. Een crisismanagementaanpak waaronder periodieke crisisoefeningen maken onderdeel uit van het BCP. Taken en verantwoordelijkheden zijn duidelijk toegewezen in het BCP. Het BCP wordt na een jaarlijkse oefening steeds geactualiseerd.

Verantwoordelijkheden:

- Directeur Bestuurder is verantwoordelijk voor het formeel goedkeuren van het bedrijfscontinuïteitsplan.
- BICT-er is verantwoordelijk voor het opstellen en het beheren van het bedrijfscontinuïteitsplan.

4.4 Back-up en herstel

Om de impact van verstoringen of dataverlies te beperken heeft Stichting SKOPOS de zorg voor back-ups van systemen en data uitbesteed bij een externe IT-partner. Op basis van de BIV-classificatie (beschikbaarheid, integriteit en vertrouwelijkheid) van systemen worden de back-upvereisten voor de systemen en de data binnen deze systemen vastgesteld. Back-ups worden regelmatig getest om te verifiëren of gegevens kunnen worden hersteld binnen de vastgestelde periode. De volgende uitgangspunten worden hierbij gehanteerd:

- De proceseigenaar is degene die beslist over de continuïteitsvereisten van een dataverwerking of een systeem. Het initiatief voor deze afweging komt van de systeemeigenaar.
- We stellen dezelfde back-upeisen aan diensten van externe leveranciers als aan systemen die we zelf beheren.
- Bij voorkeur maken we bij externe leveranciers gebruik van de back-upfaciliteit die ze zelf bij hun dienst aanbieden. Ontbreekt die of voldoet die niet, dan maken we zelf back-ups van de informatie die we verwerken in de dienst van deze leverancier.
- We evalueren jaarlijks met de IT-partner de manier waarop ze back-ups maken.

Verantwoordelijkheden:

- Stichting SKOPOS stelt een procesbeschrijving op voor back-up en herstel.
- Directeur bestuurder is verantwoordelijk voor het formeel goedkeuren van de back-up en herstel procesbeschrijving.
- BICT is verantwoordelijk voor het opstellen en het beheren van de back-up en herstel procesbeschrijving.
- De systeemeigenaar is verantwoordelijk voor het toepassen van het back-up en herstelproces.

4.5 Fysieke beveiliging

Stichting SKOPOS hanteert een losstaand Fysiek beveiligingsbeleid. Zie Reglement Cameratoezicht.

4.6 Systeem- en data-eigenaarschap en configuratiebeheer

Om IT-processen te beheren is inzicht nodig in welke systemen worden gebruikt binnen de organisatie. Veel van de IBP-thema's in dit beleid zijn afhankelijk van dit inzicht. De rol van systeemeigenaar wordt gebruikt om bepaalde verantwoordelijkheden toe te kunnen wijzen die specifiek voor een systeem gelden. De rol van proceseigenaar wordt gebruikt om bepaalde verantwoordelijkheden toe te kunnen wijzen die te maken hebben met een specifiek proces. Stichting SKOPOS maakt de keuze om eigenaarschap van data niet vast te leggen, maar zich te beperken tot het beleggen van eigenaarschap

van systemen waar deze data in is vastgelegd. Voor het vastleggen van processen en het eigenaarschap van systemen en processen treft Stichting SKOPOS de volgende maatregelen:

- Stichting SKOPOS heeft een configuratiemanagementdatabase (CMDB) waarin alle systemen, het eigenaarschap en andere benodigde eigenschappen bijgehouden worden.
- Systeemeigenaarschap wordt bepaald vóór implementatie van nieuwe systemen. De eigenaren van systemen worden vastgelegd in het CMDB.
- Proceseigenaarschap wordt bepaald en vastgelegd binnen het verwerkingsregister.

Verantwoordelijkheden:

- BICT is verantwoordelijk voor het opstellen en het beheren van de CMDB.
- De systeemeigenaar van elk systeem is verantwoordelijk voor het vastleggen van de juiste eigenschappen in de CMDB.

4.7 Classificatie van systemen en data

Om risicogestuurd beslissingen te kunnen nemen is belangrijk om per systeem het benodigde niveau van beschikbaarheid, integriteit en vertrouwelijkheid (BIV) te bepalen. De classificatie is beperkt tot systeemniveau. Stichting SKOPOS kiest ervoor om de classificatie niet per individueel dataobject toe te passen. Stichting SKOPOS heeft voor elk systeem dat opgenomen is in de CMDB een BIV-classificatie uitgevoerd. Deze BIV-classificatie wordt gebruikt om te bepalen welke maatregelen er voor het betreffende systeem geïmplementeerd moeten worden. Voor het goed toepassen van de BIV-classificatie treft Stichting SKOPOS de volgende maatregelen:

- De BIV-classificatie wordt uitgevoerd vóór de aanschaf van een nieuw systeem. Zie beleidsthema 4.11.
- De BIV-classificatie wordt vastgelegd in de CMDB.

Verantwoordelijkheden:

- De systeemeigenaar van elk systeem is verantwoordelijk voor het uitvoeren van de BIV-classificatie en het vastleggen hiervan in de verwerkersovereenkomst.
- De privacy officer is verantwoordelijk voor het controleren van de BIV-classificatie van de systemen in de verwerkersovereenkomst en het vastleggen hiervan in de CMDB.

4.8 Securitybaseline

Dit gaat in samenspraak met de IT beheerder.

Een securitybaseline voor IT-systemen wordt vastgesteld om het risico van ongeoorloofde toegang tot IT-middelen te beperken. Stichting SKOPOS maakt gebruik van het certificeringsschema ROSA als securitybaseline voor IT-systemen in eigen beheer. De securitybaseline is formeel vastgelegd, wordt periodiek geactualiseerd en wordt goedgekeurd door het schoolbestuur. De toepassing van de securitybaseline voor IT-middelen wordt periodiek beoordeeld op naleving. Afwijkingen van de baselines zijn gedocumenteerd en goedgekeurd.

Verantwoordelijkheden:

- Directeur Bestuurder is verantwoordelijk voor het formeel goedkeuren van de securitybaseline.

- De systeemeigenaar van elk systeem is verantwoordelijk voor het voldoen aan de securitybaseline en het vastleggen van afwijkingen op de baseline.

4.9 Bewustwording

Beleid en technische maatregelen zijn niet voldoende om risico's op het terrein van informatiebeveiliging en privacy uit te sluiten. De mens is hierin ook een belangrijke factor. Daarom wordt het bewustzijn van medewerkers over de verantwoordelijkheden die ze hebben voortdurend aangescherpt, zodat de kennis van bestaande risico's wordt verhoogd en veilig en verantwoord gedrag wordt aangemoedigd. Hiervoor neemt Stichting SKOPOS de volgende maatregelen:

- Er is een bewustwordingsprogramma dat twee jaarlijks herzien wordt waarin de bewustwordingsactiviteiten en de verantwoordelijkheden voor deze activiteiten beschreven worden.

Verantwoordelijkheden:

- Directeur Bestuurder is verantwoordelijk voor het formeel goedkeuren van het bewustwordingsprogramma.
- Privacy officer is verantwoordelijk voor het opstellen en het beheren van het bewustwordingsprogramma.

4.10 Incident- en problemmanagement

Incidentmanagement is het proces voor het melden van incidenten binnen de organisatie. Sommige incidenten kunnen een datalek tot gevolg hebben. Incidenten binnen de organisatie zijn nooit helemaal uit te sluiten. Een helder beschreven incidentmanagementproces is aanwezig om incidenten op tijd te herkennen en ze adequaat af te handelen. De manier waarop dat gebeurt is vastgelegd in een procesbeschrijving waarbij de volgende onderwerpen minimaal terugkomen:

- **Een centraal punt** voor het melden van incidenten**.**
- **Incidentenregister:** Binnen dit incidentenregister wordt er duidelijk onderscheid gemaakt tussen datalekken en andere type incidenten.
- **De classificatie van incidenten:** Bij elk incident moet worden vastgesteld om wat voor type incident het gaat (beveiliging, privacy, etc.)
- **De afhandeling van het incident**: Het is duidelijk wie bij welk type incident betrokken moeten worden en wie verantwoordelijk is voor het afhandelen van de incidenten.
- **Problemmanagement:** Indien incidenten regelmatig terugkomen worden deze aangemerkt als een *known error*. De procesbeschrijving beschrijft de vervolgstappen voor een terugkerend incident.
- **Monitoren en rapporteren:** Afhandeling van incidenten en problemen worden gemonitord. Hierover wordt periodiek gerapporteerd.

Verantwoordelijkheden:

- Directeur Bestuurder is verantwoordelijk voor het formeel goedkeuren van de incidentmanagementprocesbeschrijving.

- Privacy officer is verantwoordelijk voor het opstellen en het beheren van de incidentmanagementprocesbeschrijving.
- Privacy officer is verantwoordelijk voor het inrichten en beheren van het incidentenregister.

4.11 Risicomanagement leveranciers

Stichting SKOPOS besteedt een deel van de IT uit aan leveranciers, maar blijft eindverantwoordelijk voor beveiliging van informatie en persoonsgegevens. Om ervoor te zorgen dat ook leveranciers zich houden aan de technische maatregelen die volgen uit de securitybaseline zijn bepaalde stappen toegevoegd aan het leveranciersmanagementproces.

- Er is een lijst met maatregelen opgesteld op basis van de securitybaseline van Stichting SKOPOS
- Er is een leveranciersmanagementproces: Aanschaf of gebruik applicaties en software.

Verantwoordelijkheden:

- Stichting SKOPOS is verantwoordelijk voor het formeel goedkeuren van de leveranciersmanagementprocesbeschrijving.
- Privacy officer is verantwoordelijk voor het opstellen en het beheren van de leveranciersmanagementprocesbeschrijving.
- De systeemeigenaar is verantwoordelijk voor de periodieke controle op het voldoen aan de aanbestedingseisen.

4.12 Werkplekken en mobiele apparaten

Persoonsgegevens en andere informatie uit systemen die binnen onze organisatie worden gebruikt, worden ontsloten via verschillende apparaten zoals laptops, tablets, smartphones en desktop-pc's. Deze apparaten brengen risico’s met zich mee op het gebied van beveiliging, dataverlies en naleving wetgeving. Daarom treft Stichting SKOPOS de volgende maatregelen:

- Stichting SKOPOS hanteert een protocol voor het gebruik van werkplekken en mobiele apparaten.

Verantwoordelijkheden:

- Directeur Bestuurder is verantwoordelijk voor het formeel goedkeuren van de richtlijn voor het gebruik van werkplekken en mobiele apparaten.
- BICT is verantwoordelijk voor het opstellen en het beheren van de richtlijn voor het gebruik van werkplekken en mobiele apparaten.

4.13 Identiteits- en toegangsbeheer

Stichting SKOPOS maakt hiervoor een apart Identiteits- en toegangsbeleid.

4.14 Securitymanagement

Securitymanagement vormt een essentieel onderdeel voor het verminderen van risico's, het voorkomen van ongeautoriseerde toegang tot IT-systemen en het beschermen van gegevens tegen mogelijke dreigingen.

We laten ons hierin adviseren door externe partijen zoals systeembeheerder, netwerkbeheerder en werkplekbeheerder. De volgende onderdelen maken deel uit van het securitymanagement:

4.14.1 Vulnerabilitymanagement[2] en pentesting[3]

Vulnerabilitymanagement en pentesting vormen een essentieel onderdeel voor het verminderen van risico's, het voorkomen van ongeautoriseerde toegang tot IT-systemen en het beschermen van gegevens tegen mogelijke dreigingen.

4.14.2 Patchmanagement[4]

Met patchmanagement verhelp je kwetsbaarheden in systemen, applicaties en hardware. Het doel is om de beveiliging, stabiliteit en prestaties van IT-omgevingen te waarborgen door het tijdig testen en implementeren van patches.

4.14.3 Logging[5]

Loggegevens bieden inzicht in de activiteiten van systemen en spelen een sleutelrol bij het detecteren, onderzoeken en voorkomen van beveiligingsincidenten.

4.14.4 Digitaal sleutelbeheer

Met digitaal sleutelbeheer stel je encryptie in voor de volgende doeleinden:

- Bescherming van vertrouwelijke gegevens: Door het toepassen van sterke versleutelingstechnieken bij opslag, verzending en verwerking van gegevens.
- Verificatie van identiteit: Gebruik van cryptografische methoden zoals digitale handtekeningen en certificaten om betrouwbare communicatie te waarborgen.
- Waarborgen van gegevensintegriteit: Detecteren van wijzigingen in gegevens.

<u>Verantwoordelijkheden:</u>

---

[2] Vulnerabilitymanagement (Kwetsbaarheidsbeheer) is een continu, proactief proces om beveiligingslekken in IT-systemen, applicaties en netwerken te identificeren, prioriteren en verhelpen.

[3] Een pentest (penetratietest) is een gesimuleerde, geautoriseerde cyberaanval op computersystemen, netwerken of applicaties om beveiligingskwetsbaarheden op te sporen.

[4] Patchmanagement is het proces van identificeren, verkrijgen, testen en installeren van software-updates op IT-systemen om deze veilig en up-to-date te houden.

[5] Logging is een beveiligingsmaatregel. Hiermee worden gebeurtenissen in systemen vastgelegd. Bijvoorbeeld wie bepaalde gegevens heeft bekeken of aangepast en wanneer dit gebeurde. Maar ook pogingen om ongeautoriseerd toegang te krijgen.

- Directeur Bestuurder is verantwoordelijk voor het formeel goedkeuren van de procesbeschrijvingen van de onderdelen van het securitymanagement.
- IT beheerder is verantwoordelijk voor het opstellen en het beheren van de procesbeschrijvingen van de onderdelen van het securitymanagement.
- De systeemeigenaar is daar waar nodig verantwoordelijk voor tijdig testen en implementeren van beveiligingsmaatregelen.

5 Uitgangspunten privacy

Het algemene uitgangspunt in dit IBP-beleid is dat persoonsgegevens in overeenstemming met de AVG en gerelateerde wet- en regelgeving op zorgvuldige wijze worden verwerkt. Om aan dit uitgangspunt te voldoen verwerkt Stichting SKOPOS persoonsgegevens in overeenstemming met de Privacyvuistregels die in verderop in dit hoofdstuk worden uiteengezet. Stichting SKOPOS treft verdiepende maatregelen om de beleidsthema's in dit IBP-beleid in te vullen.

Persoonsgegevens

Persoonsgegevens zijn gegevens die direct of indirect over iemand gaan en dus naar een persoon te herleiden zijn, zoals een naam of e-mailadres. Naast gewone persoonsgegevens - denk aan contactgegevens en onderwijsnummers - onderscheidt de AVG bijzondere persoonsgegevens en strafrechtelijke persoonsgegevens. Daarnaast bestaat een categorie 'gevoelige' persoonsgegevens die niet expliciet in de AVG is benoemd. Dit zijn persoonsgegevens die vanwege hun aard privacygevoelig zijn en daarom extra bescherming verdienen.

- **Bijzondere persoonsgegevens** zijn gegevens die te maken hebben met bijvoorbeeld ras of etnische afkomst, gezondheid, religie of seksueel gedrag. De verwerking van deze gegevens is verboden, tenzij een wettelijke uitzondering bestaat zoals toestemming van de betrokkene.
- **Strafrechtelijke gegevens** zijn gegevens die te maken hebben met strafrechtelijke veroordelingen en strafbare feiten. De verwerking van deze gegevens is ook verboden, tenzij hiervoor een wettelijke uitzondering geldt.
- **Gevoelige persoonsgegevens** zijn gegevens die een groter privacyrisico vormen dan gewone persoonsgegevens. Denk aan financiële gegevens, burgerservicenummers (BSN), beoordelingen of gegevens van kwetsbare leerlingen.

NB: Nummers ter identificatie van een persoon, zoals het BSN, mogen alleen worden gebruikt voor specifieke doeleinden die in de wet zijn vastgelegd. Een onderwijsnummer (persoonsgebonden nummer) is gelijk aan het BSN.

Privacyvuistregels

Bij het verwerken van persoonsgegevens houdt Stichting SKOPOS rekening met onderstaande vuistregels. Door deze basisprincipes te volgen zorgen we ervoor dat we kunnen voldoen aan de AVG.

1. **We verwerken persoonsgegevens rechtmatig en transparant**

Stichting SKOPOS verzamelt en gebruikt persoonsgegevens op een eerlijke en transparante manier. Persoonsgegevens worden alleen verwerkt als daarvoor een wettelijke grondslag bestaat in de AVG. We leggen altijd duidelijk uit waarom we bepaalde gegevens nodig hebben, wat we ermee doen en hoe lang we deze gegevens bewaren. Daarom informeren we ouders en leerlingen tijdig over het gebruik van hun

persoonsgegevens, via een transparante privacyverklaring. Dit gebeurt bijvoorbeeld op het moment van inschrijving van een leerling.

2. We verwerken persoonsgegevens voor specifieke doeleinden

Stichting SKOPOS verwerkt persoonsgegevens alleen wanneer vooraf de specifieke doeleinden voor de verwerking zijn bepaald. Deze doeleinden worden vastgelegd. Persoonsgegevens worden niet voor andere, niet-verenigbare, doelen verwerkt. We zullen dus niet persoonsgegevens verzamelen omdat die wellicht ooit van pas gaan komen. We doen dit alleen met vooraf bepaalde, duidelijke en gerechtvaardigde doelen, zoals het plannen van onderwijs en communiceren met leerlingen en ouders over de voortgang en schoolactiviteiten.

3. We verwerken alleen noodzakelijke persoonsgegevens

Stichting SKOPOS verzamelt alleen persoonsgegevens die noodzakelijk zijn voor het doel waarvoor ze worden verwerkt. We vragen dus niet om meer gegevens dan we daadwerkelijk nodig hebben en hanteren hierbij het uitgangspunt 'zo min mogelijk'. We onderzoeken altijd of we met minder gegevens of enkel met anonieme gegevens kunnen werken. Zo vragen we bij de inschrijving van een leerling alleen om de gegevens die relevant zijn voor het kunnen bieden van onderwijs en bewaren we geen overbodige gegevens die niet nodig zijn voor onze schoolactiviteiten.

4. We zorgen dat persoonsgegevens juist en actueel zijn

Stichting SKOPOS treft maatregelen om ervoor te zorgen dat persoonsgegevens correct en actueel zijn. Onjuiste of achterhaalde gegevens worden geactualiseerd of verwijderd. Leerlingen en ouders kunnen op een laagdrempelige manier doorgeven dat persoonsgegevens incorrect zijn en/of gewijzigd moeten worden. Onze processen en systemen worden zo ingericht dat de juistheid van gegevens zoveel mogelijk wordt afgedwongen en gecontroleerd.

5. We bewaren persoonsgegevens niet langer dan nodig

Stichting SKOPOS bewaart persoonsgegevens niet langer dan noodzakelijk is voor het doel waarvoor ze zijn verzameld. Zodra gegevens niet meer nodig zijn, worden ze verwijderd of geanonimiseerd. We houden ons hierbij aan vooraf vastgestelde bewaartermijnen. Zo wordt het leerlingendossier (inclusief rapporten en schoolprestaties) na uitschrijving van een leerling niet langer bewaard dan nodig is voor administratieve en onderwijsdoeleinden en dus zo spoedig mogelijk verwijderd, in ieder geval binnen 2 jaar na uitschrijving.

6. We zorgen voor een passende bescherming van persoonsgegevens

We kunnen de privacy van leerlingen, ouders en medewerkers alleen goed beschermen als we op een veilige manier met hun persoonsgegevens omgaan. We zijn daarom verantwoordelijk voor het treffen van passende technische en organisatorische beveiligingsmaatregelen. Die maatregelen moeten ervoor zorgen dat de persoonsgegevens op een passende wijze worden beveiligd en worden beschermd tegen verlies, vernietiging, beschadiging of onrechtmatige verwerking. Dit doen we bijvoorbeeld door het gebruik van veilige systemen voor de opslag van leerlinggegevens en het opleiden van personeel in het veilig omgaan met gevoelige gegevens.

7. We kunnen aantonen dat we voldoen aan de AVG

We zijn verantwoordelijk voor het naleven van bovengenoemde vuistregels en kunnen daarmee aantonen dat we voldoen aan de belangrijkste uitgangspunten van de AVG. Dit doen we bijvoorbeeld

door het bijhouden van een verwerkingsregister en het uitvoeren van *Data Protection Impact Assessments* (DPIA's) [6]voor gegevensverwerkingen met een hoog privacyrisico.

8. We kunnen ons ethisch verantwoorden

Bij het beoordelen van verwerkingen van persoonsgegevens houdt Stichting SKOPOS niet alleen rekening met de vereisten uit de AVG ('*mogen we dit?*'), maar nadrukkelijk ook met ethische aspecten ('*willen we dit*?). Het gaat hierbij dus niet om de vraag of we iets 'mogen' of 'kunnen', maar juist om de vraag of we iets zouden moeten 'willen' als school. Ethische aspecten spelen in het bijzonder een rol bij verwerkingen die privacyrisico's kunnen opleveren, bijvoorbeeld bij het gebruik van meekijksoftware of schermcontroles. Dit moet ook worden bezien vanuit een ethisch afwegingskader. We stellen ons dan ook eerst de vraag of we het kunnen uitleggen aan leerlingen en ouders.

6 Beleidsthema's privacy

6.1 Verwerkingsregister

Stichting SKOPOS heeft maatregelen getroffen om aantoonbaar te voldoen aan de eisen uit de AVG. Dit houdt onder meer in dat Stichting SKOPOS kan aantonen dat de verwerking van persoonsgegevens voldoet aan de uitgangspunten uit de AVG. Stichting SKOPOS geeft onder meer invulling aan haar verantwoordingsplicht door een overzicht bij te houden met informatie over de persoonsgegevens die zij verwerkt. Dit heet het verwerkingsregister. Dit register bevat bijvoorbeeld informatie over de leerlingenadministratie of het HR-systeem. Het bijhouden van het verwerkingsregister zorgt voor een goed overzicht van welke persoonsgegevens worden verwerkt en met welk doel dit gebeurt. Het register stelt Stichting SKOPOS in staat te voldoen aan haar verantwoordingsplicht.

Het verwerkingsregister bevat van afzonderlijke verwerkingsactiviteiten informatie over onder meer de doeleinden voor de verwerking, de toepasselijke grondslag onder de AVG, een beschrijving van de betrokkenen, een beschrijving van de persoonsgegevens, de toepasselijke bewaartermijnen en de ontvangers waarmee persoonsgegevens worden gedeeld.

6.1.1 Legitiem doel en doelbinding

Persoonsgegevens worden alleen verwerkt als een specifiek, vooraf bepaald doel is vastgesteld door Stichting SKOPOS Dit doel moet duidelijk en in begrijpelijke taal aan de betrokkenen worden uitgelegd. Persoonsgegevens mogen niet voor andere doeleinden worden gebruikt.

Stichting SKOPOS verwerkt persoonsgegevens om haar verplichtingen als onderwijsinstelling na te kunnen komen. Het schoolbestuur verwerkt persoonsgegevens in de eerste plaats om onderwijs te kunnen bieden aan haar leerlingen en om activiteiten die hieraan ondersteunend zijn te kunnen uitvoeren. Hierbij valt te denken aan verwerkingen in het kader van het aanmeldproces, om te communiceren met leerlingen en ouders/verzorgers, het bijhouden van de leerlingenadministratie, het maken van roosters en om de voortgang bij te houden. Ook verwerkt het schoolbestuur

[6] Een Data Protection Impact Assessment (DPIA), in het Nederlands gegevensbeschermingseffectbeoordeling genoemd, is een verplicht onderzoek onder de AVG om privacyrisico's van gegevensverwerking vooraf in kaart te brengen. Het doel is om risico's voor betrokkenen te inventariseren en maatregelen te nemen om deze te verkleinen of te voorkomen.

persoonsgegevens van haar medewerkers in haar rol als werkgever. Stichting SKOPOS verwerkt bij deze werkzaamheden verschillende (categorieën) persoonsgegevens, waaronder contactgegevens, naam, geboortedatum en gegevens betreffende de aard en het verloop van het onderwijs. Stichting SKOPOS verwerkt deze persoonsgegevens op basis van grondslagen uit de AVG, bijvoorbeeld omdat sprake is van een wettelijke taak of verplichting, een gerechtvaardigd belang of op basis van toestemming.

Als gegevens toch voor een ander doel nodig zijn, dan mag dit alleen als dat doel verenigbaar is met het oorspronkelijke doel. Om te bepalen of dit het geval is, moet onder andere worden gekeken naar:

- De relatie tussen het nieuwe en het oorspronkelijke doel.
- De context waarin de gegevens zijn verzameld en de redelijke verwachtingen van de betrokkenen.
- Het soort persoonsgegevens; gevoelige gegevens verdienen extra bescherming.
- De mogelijke gevolgen voor betrokkenen.
- Bescherming van de gegevens, zoals versleuteling of pseudonimiseren.

Voor elke nieuwe verwerking moet Stichting SKOPOS de rechtmatigheid, zorgvuldigheid en noodzaak opnieuw beoordelen. De specifieke doeleinden worden voorafgaand aan de verwerking bepaald en vermeld in de privacyverklaring om betrokken te informeren. Ook worden de doeleinden opgenomen in het verwerkingsregister. Voordat gegevens voor een ander doel worden gebruikt, vindt overleg plaats met de privacy officer en indien nodig ook met de functionaris gegevensbescherming.

6.1.2 Grondslag

Stichting SKOPOS moet voor iedere verwerking van persoonsgegevens een geldige reden hebben. De AVG noemt dit een grondslag. Stichting SKOPOS verwerkt persoonsgegevens alleen op basis van de in de AVG genoemde grondslagen:

- de betrokkene heeft **toestemming** verleend, bijvoorbeeld voor het maken en delen van foto's of video's.
- de verwerking is noodzakelijk voor de **uitvoering van een overeenkomst** waarbij de betrokkene partij is, bijvoorbeeld het verwerken van salaris om de arbeidsovereenkomst met werknemers na te komen.
- de verwerking is noodzakelijk om te voldoen aan een **wettelijke verplichting,** bijvoorbeeld het delen van salarisinformatie met de Belastingdienst voor de uitvoering van de belastingwetgeving.
- de verwerking is noodzakelijk om **de vitale belangen** van de betrokkene te beschermen, bijvoorbeeld bij een levensbedreigende situatie waarbij het noodzakelijk is dat bepaalde gegevens van een leerling acuut aan hulpverleners moeten worden doorgeven.
- de verwerking is noodzakelijk om uitvoering te geven aan een **taak van algemeen belang**, hierbij gaat het om wettelijk vastgestelde taken en bevoegdheden**.** Zo heeft Stichting SKOPOS de wettelijke taak om onderwijs te bieden.
- de verwerking is noodzakelijk voor de behartiging van een **gerechtvaardigd belang** van Stichting SKOPOS of van een derde. Denk hierbij aan het verwerken van medewerkersgegevens voor het opstellen van managementrapportages ten behoeve van beleidsontwikkeling of het gebruik van bewakingscamera's op het schoolplein.

De toepasselijke grondslag wordt vooraf vastgesteld, bijvoorbeeld middels een DPIA, en benoemd in de privacyverklaring om betrokken te informeren. Ook wordt de toepasselijke grondslag opgenomen in het verwerkingsregister.

6.2 Informatieplicht

Stichting SKOPOS verwerkt persoonsgegevens op een behoorlijke en transparantie manier. Dit is in begrijpelijke taal inzichtelijk voor de betrokkenen. Stichting SKOPOS informeert leerlingen en medewerkers voorafgaand aan de gegevensverwerking op transparante wijze via een duidelijke privacyverklaring. Deze privacyverklaring wordt gepubliceerd op de website. Daarnaast informeert de school medewerkers en sollicitanten ook via een aparte privacyverklaring. Hiermee zorgt Stichting SKOPOS ervoor dat betrokkenen weten welke persoonsgegevens worden verwerkt en voor welke doeleinden dit gebeurt. Ook zijn ze op de hoogte van de rechten die ze hebben.

Wordt gebruik gemaakt van geautomatiseerde besluitvorming of profilering? Dan gelden extra strenge regels, ook op het gebied van transparantie. Dat betekent onder andere dat medewerkers en leerlingen goed moeten worden geïnformeerd over het gebruik hiervan en duidelijk moet worden uitgelegd op basis van welke criteria het besluit tot stand is gekomen. Ook moet de mogelijkheid bestaan een nieuw besluit te nemen waarbij een mens de gegevens beoordeelt. Op die manier beschermen we medewerkers en leerlingen tegen onrechtmatige verwerking.

6.3 Toestemming

Bij het gebruik van toestemming als grondslag gelden een aantal voorwaarden:

- Toestemming moet op een begrijpelijke en toegankelijke manier worden gevraagd, in duidelijke taal en niet verborgen in algemene voorwaarden of lange teksten.
- Toestemming moet vrijwillig worden gegeven en moet ook weer gemakkelijk ingetrokken kunnen worden.
- Stichting SKOPOS moet kunnen aantonen dat toestemming is verkregen, bijvoorbeeld door logs of ondertekende formulieren.
- Voor kinderen onder de 16 jaar moet een wettelijke vertegenwoordiger toestemming geven. Dit geldt ook voor personen onder curatele, bewind of mentorschap. Stichting SKOPOS verifieert of deze vertegenwoordiger daadwerkelijk toestemming heeft gegeven.

Leerlingen (of hun wettelijke vertegenwoordigers) worden in bepaalde situaties om toestemming gevraagd. Denk aan de situatie dat Stichting SKOPOS foto's of video's van leerlingen maakt en publiceert. Dit mag alleen als de school vooraf toestemming heeft verkregen. Omdat een gezagsrelatie bestaat tussen Stichting SKOPOS en haar leerlingen en medewerkers, moet goed worden beargumenteerd waarom toestemming in specifieke gevallen in vrijheid kan worden gegeven. Stichting SKOPOS gaat daarom terughoudend om met het gebruik van deze grondslag. Voordat toestemming als grondslag wordt gebruikt, vindt overleg plaats met de privacy officer en indien nodig ook met de functionaris gegevensbescherming.

6.4 Privacy by design en privacy by default

Privacy by design betekent dat Stichting SKOPOS bij de ontwikkeling, het ontwerp, de selectie en het gebruik van toepassingen, diensten en producten zo vroeg mogelijk rekening houdt met privacyrisico's en passende waarborgen inbouwt om de privacy van betrokkenen te beschermen. Neemt Stichting

SKOPOS bijvoorbeeld een leerlingvolgsysteem in gebruik? Dan moet in een vroeg stadium al worden nagedacht over passende toegangsbeperkingen. Leraren horen alleen inzicht te krijgen in de noodzakelijke gegevens van hun eigen leerlingen. *Privacy by default* betekent dat de standaardinstellingen van een product, dienst of proces op de meest privacyvriendelijke instelling staan. Maakt Stichting SKOPOS bijvoorbeeld een profiel aan op sociale media? Dan mag dit profiel niet standaard openbaar zichtbaar zijn.

Hiermee zorgt Stichting SKOPOS ervoor dat zo vroeg mogelijk rekening wordt gehouden met privacybeginselen en op die manier privacyrisico's tijdig worden gemitigeerd.

6.4.1 Dataminimalisatie

Stichting SKOPOS verzamelt alleen gegevens die noodzakelijk zijn voor het doel dat voorafgaand aan de verwerking is vastgesteld. De verzamelde gegevens dienen toereikend, ter zake dienend en niet bovenmatig te zijn. Hiermee voorkomt Stichting SKOPOS dat te veel gegevens worden verwerkt. Bij de aanmelding van een leerling verzamelt Stichting SKOPOS bijvoorbeeld alleen de informatie die nodig is om de leerling op de juiste manier in te schrijven. Denk aan naam, geboortedatum, adres en contactgegevens van ouders/verzorgers. Extra informatie, zoals het beroep van de ouders, is niet relevant voor de inschrijving en hoort daarom niet te worden verzameld. Daarnaast moet de verwerking van persoonsgegevens op de minst ingrijpende wijze plaatsvinden. Als het beoogde doel op een privacyvriendelijkere manier kan worden bereikt, dan kiest Stichting SKOPOS hiervoor. Op deze manier voldoet Stichting SKOPOS eveneens aan de principes van *privacy by design*.

6.5 Bewaartermijnen

Persoonsgegevens worden niet langer bewaard dan noodzakelijk voor de doeleinden waarvoor zij zijn verzameld. Dit gebeurt in overeenstemming met het bewaar- en vernietigingsbeleid van Stichting SKOPOS. Na het verlopen van de toepasselijke bewaartermijnen zorgt Stichting SKOPOS ervoor dat persoonsgegevens tijdig worden vernietigd (of geanonimiseerd). Hierdoor worden persoonsgegevens beter beschermd tegen onnodige verwerking en datalekken. Zo worden bijvoorbeeld overzichten van schoolprestaties en rapporten uiterlijk tot 2 jaar na uitschrijving van een leerling bewaard. Het schooladvies wordt tot uiterlijk 5 jaar na uitschrijving van een leerling bewaard.

6.6 Afhandelen van datalekken

Voorbeelden van datalekken zijn een gestolen laptop, een verloren usb-stick, of een e-mail met persoonsgegevens die naar de verkeerde persoon is verstuurd. Datalekken moeten direct worden gemeld via ***Intranet-organisatie-ICT&privacy-melden incident of datalek,*** geregistreerd in het interne register voor beveiligingsincidenten en datalekken. Melden kan ook via ***privacy@skoposschijndel.nl*** Risicovolle datalekken moeten worden gemeld aan de Autoriteit Persoonsgegevens en ook aan de betrokkenen als het datalek waarschijnlijk een hoog risico voor hen oplevert. De privacy officer beoordeelt of zo'n melding nodig is. Dit gebeurt als het nodig is in samenspraak met de functionaris gegevensbescherming.

6.7 Data Protection Impact Assessment

Voor elke nieuwe verwerking van persoonsgegevens, bijvoorbeeld een nieuw proces, technologie of applicatie, controleert Stichting SKOPOS of de privacybeginselen uit de AVG worden nageleefd. Bij

verwerkingen met een hoog privacyrisico wordt eerst een *Data Protection Impact Assessment* (DPIA) uitgevoerd. Een DPIA brengt in kaart hoe groot de kans is dat de privacy van betrokkenen wordt geschaad, waar de risico's liggen en welke gevolgen dit kan hebben. Op basis van de uitkomsten van de DPIA neemt Stichting SKOPOS maatregelen om deze risico's te mitigeren.

6.8 Uitwisseling persoonsgegevens

Een verwerker is een partij die in opdracht van Stichting SKOPOS persoonsgegevens verwerkt, zoals een leverancier van een leerlingadministratiesysteem. Als Stichting SKOPOS een verwerker inschakelt om persoonsgegevens te verwerken, dan worden privacyafspraken vastgelegd in een verwerkersovereenkomst. Bepaalt Stichting SKOPOS samen met één of meerdere partijen het doel en middelen voor de verwerking van persoonsgegevens? Dan is sprake van een zogenaamde gezamenlijke verwerkingsverantwoordelijkheid. In dat geval worden ook contractuele afspraken gemaakt rondom de zorgvuldige en veilige verwerking van gegevens.

Persoonsgegevens kunnen ook beschikbaar worden gesteld aan partijen die niet als verwerkers worden aangemerkt, maar als ‘derden’. Deze derden verwerken persoonsgegevens niet in opdracht van een verwerkingsverantwoordelijke, maar voor hun eigen doel. Een verwerkersovereenkomst is daarom ook niet nodig, maar er moet wel een grondslag bestaan om de persoonsgegevens te delen. Denk aan de situatie waarin Stichting SKOPOS gegevens over medewerkers deelt met de Belastingdienst ten behoeve van de loonaangifte. De Belastingdienst verwerkt deze gegevens voor haar eigen wettelijke doeleinden en handelt niet als verwerker.

6.8.1 Gegevensverwerking buiten de EER[7]

Schakelt Stichting SKOPOS een verwerker in uit een land buiten de Europese Economische Ruimte (EER) dat geen passend beschermingsniveau biedt? Dan gelden aanvullende voorwaarden. Bij een gegevensdeling buiten de EER moeten namelijk (juridische, technische en organisatorische) waarborgen zijn genomen om het beschermingsniveau ook buiten de EER te laten voldoen aan de AVG, zodat de persoonsgegevens voldoende beschermd blijven. Om dit te bereiken wordt de verwerkersovereenkomst ook gecontroleerd door Stichting SKOPOS of de verwerker gebruik maakt van de Europese modelcontracten, de zogenaamde ‘Standard Contractual Clauses’, en neemt Stichting SKOPOS aanvullende risicogebaseerde beveiligingsmaatregelen. Ook vindt voorafgaand aan de gegevensdeling afstemming plaats met de privacy officer en afdeling informatiebeveiliging om te beoordelen of de getroffen maatregelen voldoende zijn.

NB: De bepalingen van de meest recente versie van het convenant ‘Digitale onderwijsmiddelen en privacy’ zijn leidend bij het maken van afspraken met leveranciers, die als verwerkers in opdracht van de school persoonsgegevens verwerken.

6.9 Rechten van betrokkenen

Betrokkenen hebben op grond van de AVG recht op controle op de verwerking van hun persoonsgegevens. Een betrokkene kan onder andere gebruikmaken van het recht op inzage,

[7] De term EER staat voor de Europese Economische Ruimte. Dit is een samenwerkingsverband waarmee de EU-lidstaten, samen met IJsland, Liechtenstein en Noorwegen, toegang hebben tot de interne markt van de Europese Unie. Het waarborgt het vrije verkeer van personen, goederen, diensten en kapitaal tussen deze landen.

rectificatie, verwijdering en bezwaar. Leerlingen/ouders, leraren en andere medewerkers kunnen een verzoek tot uitoefening van deze rechten indienen via: ***privacy@skoposschijndel.nl***.
Ook hebben betrokkenen het recht een klacht in te dienen bij de Autoriteit Persoonsgegevens.

Stichting SKOPOS draagt er zorg voor dat de informatie over het uitoefenen van deze rechten op een transparante manier is verstrekt aan betrokkenen via een privacyverklaring. Stichting SKOPOS zal binnen de wettelijke termijnen, uiterlijk binnen één maand, schriftelijk reageren op het verzoek. In uitzonderlijke situaties kan de reactietermijn worden verlengd, maar dan wordt dit wel binnen een maand gecommuniceerd. Voor AVG-verzoeken geldt een identificatieplicht, zodat de identiteit van de verzoeker kan worden vastgesteld. Hiertoe kan Stichting SKOPOS om extra informatie verzoeken, maar zal hierbij terughoudend zijn met het verzoeken om een kopie identiteitsbewijs.

7 Verantwoording IBP

7.1 Naleving AVG

Er vindt toezicht plaats door Stichting SKOPOS op de naleving van de normen uit dit beleid. Van belang is dat leidinggevenden hun verantwoordelijkheid nemen en medewerkers aanspreken in geval van tekortkomingen. Stichting SKOPOS besteedt in dit verband actief aandacht aan informatiebeveiliging en privacy bij de aanstelling van medewerkers, tijdens functioneringsgesprekken en via bewustwordingscampagnes.
Mocht de naleving van dit beleid ernstig tekortschieten, dan kan Stichting SKOPOS de betrokken verantwoordelijke medewerkers maatregelen opleggen binnen de kaders van de CAO en toepasselijke wetgeving. Voor toezicht op de naleving van de AVG vervult de functionaris gegevensbescherming (FG) een belangrijke rol. De FG kan bijvoorbeeld informatie verzamelen over gegevensverwerkingen en beoordelen of deze aan de AVG voldoen. Ook kan de FG adviezen en aanbevelingen verschaffen aan Stichting SKOPOS

7.2 Rapportage

Stichting SKOPOS heeft de verantwoordelijkheid om het IBP-beleid formeel goed te keuren en te monitoren of het IBP-beleid door de organisatie wordt toegepast. Jaarlijks wordt hierover gerapporteerd in het bestuursverslag.

7.3 Beleidsherziening

Het IBP-beleid wordt door Stichting SKOPOS eenmaal per 3 jaar getoetst en indien nodig herzien. Bij een substantiële wijziging van het IBP-beleid of in geval van belangrijke ontwikkelingen of veranderingen in wet- en regelgeving, volgt er indien nodig een beleidswijziging.

Bijlage 1 Overzicht vastgestelde documenten

(Code verwijst naar normen van het Normenkader IBP voor het onderwijs.)

Bijlage 2 Lijst met afkortingen

Onderstaande afkortingen komen voor in dit document.

Afkorting	Volledige naam
AVG	Algemene Verordening Gegevensbescherming
BCP	Bedrijfscontinuïteitsplan
BIA	Business Impact Analyse
BICT	Bovenschools ICT
BIV	Beschikbaarheid, Integriteit en Vertrouwelijkheid
BSN	Burgerservicenummer
CAO	Collectieve Arbeidsovereenkomst
CMDB	Configuratiemanagementdatabase
DPIA	Data Protection Impact Assessment
EER	Europese Economische Ruimte
FG	Functionaris Gegevensbescherming
GMR	Gemeenschappelijke Medezeggenschapsraad
GRC	Governance, Risk & Compliance (Bestuur, Risico en naleving)
HR	Human Resources
IBP	Informatiebeveiliging en Privacy
ROSA	Referentie Onderwijs Sector Architectuur
UAVG	Uitvoeringswet Algemene verordening gegevensbescherming