



Privacyreglement SKOVV

1. Inleiding

Informatie en ict zijn noodzakelijk in het onderwijs. Omdat we met die informatie en ict ook persoonsgegevens verwerken, is de **Algemene verordening gegevensbescherming** (hierna: AVG) daarop van toepassing. De AVG bepaalt onder welke voorwaarden persoonsgegevens gebruikt mogen worden en dat er passende technische en organisatorische maatregelen genomen moeten worden om de persoonsgegevens te beschermen.

Stichting Katholiek Onderwijs Veluwe-Vallei (hierna: SKOVV) vindt de privacy van haar leerlingen, ouders en medewerkers erg belangrijk en gaat daarom zorgvuldig om met de verwerking van hun persoonsgegevens.

Dit reglement beschrijft hoe de SKOVV omgaat met de verwerkingen van persoonsgegevens en de beveiliging van de informatie. Het is bedoeld als centrale informatiebron voor alle betrokkenen.

Per categorie betrokkene (leerlingen en hun ouders, medewerkers, derden) leest u hierin terug om wat voor soort persoonsgegevens het gaat, wat het doel en de grondslag van de verwerking is, wat het toegangs- en beveiligingsbeleid is en in hoeverre de persoonsgegevens met derden worden gedeeld. Ook leest u in dit privacyreglement hoe lang SKOVV persoonsgegevens bewaart en welke rechten u heeft onder de AVG.

Met dit privacyreglement voldoet de SKOVV aan de informatieplicht uit de AVG. Het reglement wordt jaarlijks herzien.

2. Privacy van leerlingen en hun ouders

2.1. Om wat voor soort persoonsgegevens gaat het?

Van leerlingen en hun ouders verzamelen wij (zowel digitaal als op papier) de volgende categorieën persoonsgegevens:

- NAW- en contactgegevens
- Geboortedatum
- Culturele achtergrond
- Hoogst genoten opleiding ouders
- Administratienummer (o.a. BSN)
- Ontwikkelingsvoortgang en leerresultaten
- Gezondheidsgegevens (bijv. dyslexie)
- Verzuimgegevens

- Administratieve gegevens (bijv. in welk klas uw kind zit, het rooster, etc)
- Beeldmateriaal
- Gegevens die nodig zijn voor het berekenen, vastleggen en innen van inschrijvingsgelden, school- en les-gelden en bijdragen of vergoedingen voor leermiddelen en buitenschoolse activiteiten
- Loggegevens over gebruik van systemen

2.2. Wat zijn de doelen en grondslagen van de verwerkingen?

De persoonsgegevens worden verzameld om:

- te voldoen aan wettelijke verplichtingen
- leerlingen toe te laten op school
- bekostiging te ontvangen van de overheid
- te communiceren met leerlingen en ouders
- PR-doeleinden
- onderwijs te organiseren
- onderwijs uit te voeren / af te stemmen op de ontwikkeling van de leerling
- leerlingen extra ondersteuning/begeleiding te bieden
- administratie- en financieel beheer doeleinden
- de systemen te beveiligen, toegang daartoe mogelijk te maken, te controleren en misbruik/oneigenlijk gebruik te voorkomen
- De continuïteit en goede werking van de systemen te waarborgen

De persoonsgegevens van leerlingen worden verzameld op grond van een wettelijke verplichting, de toestemming van ouders/verzorgers (bijv. de verwerking van beeldmateriaal) of op grond van een gerechtvaardigd belang van SKOVV.

2.3 Toegang en beveiliging

Binnen de school hebben de volgende medewerkers (rollen) toegang tot persoonsgegevens van leerlingen:

- Leden van de directie en het MT
- Onderwijzend personeel
- Onderwijsondersteunend personeel (OOP: administratief, zorg coördinator, IB, ict-ondersteunend)

Niet alle rollen hebben tot alle gegevens toegang. Per rol is in een toegangsmatrix vastgesteld welke gegevens die rol mag inzien (leesrechten) en welke gegevens die rol mag wijzigen (schrijfrechten). Het toegangsbeleid wordt jaarlijks gecontroleerd. De toegangsmatrix staat in het privacyhandboek.

Papieren dossiers die persoonsgegevens van leerlingen bevatten, worden in afgesloten kasten bewaard. Alleen de medewerkers die deze persoonsgegevens nodig hebben om hun werk goed te kunnen doen, hebben toegang tot die kasten.

Gegevens met betrekking tot administratie, inschrijving, onderwijsbegeleiding en zorg worden in het leerlingvolgsysteem ParnasSys opgeslagen. Inloggen tot ParnasSys is alleen voorbehouden aan medewerkers die in dienst zijn van het bestuur en in incidentele gevallen voor externe zorgbegeleiders. Met de leverancier van ParnasSys is een zogenaamde

verwerkersovereenkomst (conform het model van de PO-raad) afgesloten, waarin ook afspraken zijn gemaakt over beveiliging en backup van de data die in ParnasSys wordt opgeslagen. ParnasSys voldoet aan de nationale standaarden op het gebied van beveiliging die de overheid heeft bepaald. Als de school gegevens moet uitwisselen met andere scholen of de overheid, dan gebeurt dit via het beveiligde ParnasSys. Met de externe zorgbegeleider zijn ook privacy-afspraken gemaakt.

Voor digitale leermiddelen en toetsen worden systemen van diverse leveranciers of uitgeverijen gebruikt. Met deze partijen zijn eveneens verwerkersovereenkomsten afgesloten. Onderdeel hiervan is dat zij ook voldoen aan de nationale standaarden en voorzieningen met betrekking tot de veilige uitwisseling van persoonsgegevens. In dit kader wordt gebruik gemaakt van de nummervoorziening die het mogelijk maakt om alleen nog maar gepseudonimiseerde gegevens met deze partijen uit te wisselen. Meer informatie hierover is [hier](#) te vinden.

2.4. Worden de persoonsgegevens met derden gedeeld?

De persoonsgegevens van leerlingen worden **niet** met derden gedeeld zonder toestemming van de ouders, tenzij de school wettelijk verplicht is om bepaalde persoonsgegevens te verstrekken.

Zo heeft de school bijvoorbeeld wettelijke verplichtingen om persoonsgegevens te delen met het samenwerkingsverband, de Inspectie, leerplichtambtenaar, DUO enz.

De meest voorkomende gevallen waarin de school toestemming aan ouders vraagt om persoonsgegevens met derden te delen, zijn de situaties waarin de school een externe expert wil benaderen voor aanvullende onderwijs- en zorgbegeleiding voor de leerling. Denk aan een schoolmaatschappelijk werker, schoolarts, orthopedagoog, ambulante begeleider, remedial teacher. Toestemming van ouders wordt schriftelijk gevraagd en opgeslagen in het leerlingdossier.

3. Privacy van medewerkers

3.1 Om wat voor soort persoonsgegevens gaat het?

- NAW- en contactgegevens;
- Persoonsgegevens die op het identiteitsbewijs staan (o.a. BSN)
- Salarisgegevens waaronder IBAN
- Gegevens over functioneren, loopbaan en benoeming
- Gegevens over een evt. justitieel verleden
- Verzuim- en verlofgegevens
- Gezondheidsgegevens i.v.m. arbo
- Gegevens over de klas waaraan een medewerker gekoppeld is
- Loggegevens over het gebruik van de systemen

3.2 Wat zijn de doelen en grondslagen van deze verwerkingen?

Deze gegevens worden verzameld om:

- Personeel aan te nemen en te ontslaan
- Personeel (bege)leiding en bijscholing te geven
- Te voldoen aan (fiscaal) wettelijke verplichtingen
- Personeelsadministratie en -beleid te voeren
- Loon uit te betalen
- Arbeidsvoorwaarden uit te kunnen voeren
- Medewerkers bij te kunnen scholen
- Interne controle, accountantscontrole en bedrijfsvoering
- Personeel toegang te geven tot het leerlingvolgsysteem met bijbehorende autorisaties
- Personeel te laten werken met digitale onderwijsmiddelen
- de systemen te beveiligen, controleren en misbruik/oneigenlijk gebruik te voorkomen
- De continuïteit en goede werking van de systemen te waarborgen

De persoonsgegevens worden verzameld op de grondslag van een wettelijke verplichting, het uitvoeren van een overeenkomst of toestemming van medewerkers.

3.3 Toegang en beveiliging

Medewerkers kunnen sinds 1 juli 2019 hun eigen digitale personeelsdossier inzien in You Force met behulp van hun eigen inlog. Binnen SKOVV hebben voorts de volgende medewerkers (rollen) toegang tot persoonsgegevens van medewerkers:

- De bestuurder
- Administratief personeel stafbureau
- Medewerkers salarisadministratie en financiën administratiekantoor
- Personeelsfunctionaris SKOVV
- Leidinggevende van de betreffende medewerker
- ICT-ondersteunend personeel

Niet alle rollen hebben tot alle gegevens toegang. Per rol is vastgesteld welke gegevens die rol mag inzien (leesrechten) en wijzigen (schrijfrechten). Het toegangsbeleid wordt jaarlijks gecontroleerd. Voor personeelsgegevens die in dezelfde systemen worden verwerkt als die van leerlingen, gelden dezelfde beveiligingsmaatregelen uit paragraaf 2.3.

Via Camas worden verzuimgegevens geregistreerd. Ook hiervoor geldt dat er binnen het bestuur een toegangsbeleid is opgesteld dat jaarlijks wordt gecontroleerd. Met Camas ook verwerkersovereenkomsten afgesloten. Toegang tot medische gegevens komt tot stand tussen Camas en medische specialisten (arboarts/arbeidsdeskundige) zonder tussenkomst van het bestuur.

3.4 Worden de persoonsgegevens met derden gedeeld?

SKOVV deelt persoonsgegevens van medewerkers **niet** met derden zonder toestemming van de betreffende medewerker, tenzij de school wettelijk verplicht is om bepaalde persoonsgegevens te verstrekken.

4. Privacy van derden

In deze categorie gaat het om vrijwilligers, sollicitanten, extern ingehuurd personeel en oud-leerlingen.

4.1. Om wat voor soort persoonsgegevens gaat het?

- NAW- en contactgegevens
- Betaalgegevens
- Gegevens over een eventueel justitieel verleden
- Studie- en loopbaangegevens
- Persoonsgegevens op het ID-bewijs zoals BSN (in geval van een externe professional)

4.2. Wat zijn de doelen en grondslagen voor de verwerkingen?

Deze gegevens worden verzameld om:

- De geschiktheid van een sollicitant te beoordelen
- De veiligheid binnen de organisatie te borgen
- De door de sollicitant gemaakt onkosten af te handelen
- Inkomende facturen te betalen
- Externen toegang geven tot ICT en software die nodig zijn bij het uitvoeren van hun taak
- Te voldoen aan wettelijke verplichtingen
- Te communiceren met vrijwilligers, oud-leerlingen en hun ouders, externe professionals

De grondslagen voor deze verwerkingen zijn toestemming, uitvoeren van een overeenkomst of gerechtvaardigd belang.

4.3 Toegang en beveiliging

De persoonsgegevens van sollicitanten kunnen alleen worden ingezien door medewerkers die betrokken zijn bij de sollicitatieprocedure.

De persoonsgegevens van externen kunnen worden geraadpleegd door medewerkers administratie, personeelsadviseurs, hoofd P&O en ICT-ondersteunend personeel.

De persoonsgegevens van vrijwilligers en oud-leerlingen kunnen alleen worden geraadpleegd door medewerkers administratie.

4.4. Worden de persoonsgegevens ook met derden gedeeld?

De persoonsgegevens van sollicitanten worden alleen verstrekt aan externe partijen die namens het bestuur een test of assessment verzorgen. In dat geval worden slechts die persoonsgegevens verstrekt die noodzakelijk zijn voor de test of assessment.

5. Bewaartermijnen

Gegevens	Bewaartermijn
Gegevens over verzuim en afwezigheid	Maximaal 5 jaar nadat een leerling is uitgeschreven
Gegevens in- en uitschrijving (noodzakelijk voor berekening van bekostiging)	Maximaal 5 jaar nadat een leerling is uitgeschreven
Gegevens die nodig zijn om te berekenen hoeveel bekostiging de school krijgt	Minimaal 7 jaar na afloop van het schooljaar waarop de bekostiging betrekking heeft
Gegevens in het leerlingdossier	Maximaal 2 jaar nadat een leerling is uitgeschreven
Gegevens met betrekking tot bezwaar-, klachten- of gerechtelijke procedure.	Maximaal 5 jaar nadat leerling is uitgeschreven
Camerabeelden t.b.v. toezicht	Maximaal 4 weken, tenzij er een incident is vastgelegd.
Gegevens in personeelsdossier met betrekking tot fiscale bewaarplicht	Maximaal 5 jaar na uitdiensttreding
Overige gegevens in het personeelsdossier	Maximaal 2 jaar na uitdiensttreding
Gegevens over het gebruik van ICT-middelen en het schoolnetwerk door personeel en leerlingen	Maximaal 6 maanden
Sollicitatiebrief, formulier, correspondentie omtrent de sollicitatie, getuigschriften, verklaring omtrent gedrag, psychologisch onderzoek	Maximaal 4 weken zonder toestemming, maximaal 1 jaar met toestemming van de sollicitant, maximaal 2 jaar na uitdiensttreding voor benoemde collega.

6. Datalekken

Wanneer de kans bestaat dat er persoonsgegevens in handen zijn gekomen van derden die geen toegang zouden moeten hebben tot die gegevens of wanneer de mogelijkheid bestaat dat er persoonsgegevens verloren zijn gegaan dient dit direct gemeld te worden via de procedure melden datalekken van SKOVV. Het bevoegd gezag is verantwoordelijk voor eventuele melding van een datalek bij de Autorisatie Persoonsgegevens, indien er onterecht geen melding gedaan wordt kan dit leiden tot fikse boetes. De volledige procedure melden datalekken is opgenomen in het privacyhandboek.

7. Rechten van betrokkenen

De AVG geeft ouders, medewerkers en andere betrokkenen het recht op inzage in en aanpassing/verwijdering van hun persoonsgegevens. Ook hebben zij recht op beperking van de verwerking van hun persoonsgegevens, het recht om bezwaar te maken tegen de verwerking van hun persoonsgegevens en het recht om de digitale persoonsgegevens te ontvangen die SKOVV van hen heeft. Heeft u toestemming gegeven voor een bepaalde verwerking van persoonsgegevens, zoals toestemming voor het gebruik van beeldmateriaal van uw kind? Dan mag u deze toestemming te allen tijde weer intrekken.

U kunt uw rechten uitoefenen door een e-mail te sturen naar de privacy@skovv.nl. De contactgegevens staan hieronder. De SKOVV zal uw verzoek binnen de wettelijke termijn afhandelen voor zover dit redelijkerwijs mogelijk is. Medewerkers kunnen hun eigen personeelsdossier bovendien inzien door middel van de persoonlijke inlog die zij daarvoor hebben ontvangen.

Heeft u verder nog een vraag, wilt u een overzicht opvragen van de leveranciers/uitgeverijen met wie SKOVV een verwerkersovereenkomst heeft afgesloten of vindt u dat het privacyreglement niet op de juiste wijze wordt nageleefd binnen het bestuur? Dan mag u natuurlijk ook een e-mail sturen. Als u niet tevreden bent over de reactie dan kunt u zich wenden tot het bestuur. Leidt ook dit niet tot een oplossing? Dan kunt u een klacht indienen bij de Autoriteit Persoonsgegevens.

8. Contactgegevens

Stichting Katholiek Onderwijs Veluwe-Vallei (SKOVV)
KVK 41051103
Groenendaal 7
6715 BA Ede
FG: privacy@skovv.nl