



VO Veghel
Fioretti College & Zwijsen College

Reglement Privacy

VO Veghel

2025-2027

Datum akkoord directie: 29-09-2025

Datum akkoord MR: 25-11-2025

Start herziening: september 2027

Inhoudsopgave

Inhoudsopgave.....	3
1 Inleiding.....	5
1.1 Begripsbepaling	5
1.1.1 Privacy	5
1.1.2 Persoonsgegevens.....	5
1.1.3 Verwerking.....	5
1.1.4 Informatiebeveiliging.....	6
1.1.5 Bestand	6
1.1.6 Autoriteit Persoonsgegevens	6
1.2 Reikwijdte	6
1.3 AVG	7
1.3.1 Grondslagen.....	8
2 Werkwijze VO Veghel	10
2.1 Grondslagen en soorten gegevens	10
2.2 Rechten en klachten	11
2.3 Doelen	11
2.4 Juistheid	11
2.4.1 Regelmatige controle en actualisatie van gegevens	11
2.4.2 Geautomatiseerde systemen.....	12
2.5 Bewaartermijnen	12
2.6 Beveiliging van gegevens	12
2.6.1 Functionarissen en beleid.....	12
2.6.2 Digitale en fysieke beveiliging.....	13
2.6.3 Beperking van toegang en verantwoordelijkheid.....	13
2.6.4 Risicoclassificaties en risicoanalyses.....	13
2.6.5 Beveiligingsincidenten en datalekken melden en registreren.....	13
3 Evaluatie	15
Bronnen	16

Bijlagen	17
Bijlage 1 Gegevens aanmeldformulier.....	17
Bijlage 2 Gegevens overdrachtsformulier.....	19

1 Inleiding

Dit is het Reglement Privacy VO Veghel 2025-2027. Dit reglement beschrijft hoe VO Veghel omgaat met persoonsgegevens van alle betrokkenen, waaronder ten minste: medewerkers, leerlingen, ouders/verzorgers, samenwerkingspartners en leveranciers. Het reglement volgt de regels van de Algemene Verordening Gegevensbescherming (AVG) en ligt in het verlengde van het Beleid Privacy en het privacybeleid van OMO.

In dit reglement leest u eerst een uitleg van een aantal begrippen en van wat de AVG inhoudt. U leest daarna over de doelen van de gegevensverwerking, welke gegevens worden verwerkt, wie toegang heeft tot de gegevens, welke rechten u heeft als betrokkene, wat de klachtenprocedure is en hoe de gegevens worden beveiligd en gedeeld. Tot slot leest u hoe het reglement periodiek wordt geëvalueerd en aangepast.

1.1 Begripsbepaling

1.1.1 Privacy

Privacy betreft de bescherming van persoonsgegevens (zie [paragraaf 1.1.2](#)) (Kennisset z.d.b).

1.1.2 Persoonsgegevens

Persoonsgegevens zijn alle gegevens die iets vertellen over een persoon waardoor die persoon direct of indirect kan worden geïdentificeerd. Voorbeelden zijn: een naam, een identificatienummer, locatiegegevens, een online identifier en elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon (AVG art. 4). Er bestaat een verschil tussen gewone en bijzondere persoonsgegevens. Gewone persoonsgegevens zijn bijvoorbeeld naam, adres en mailadres. Bijzondere persoonsgegevens zijn persoonsgegevens die zo privacygevoelig zijn dat de verwerking (zie [paragraaf 1.1.3](#)) van deze gegevens een grote(re) impact kan hebben op een persoon dan de verwerking van gewone persoonsgegevens (Autoriteit Persoonsgegevens z.d.a). Voorbeelden zijn: medische gegevens en geloof.

1.1.3 Verwerking

Verwerking is een bewerking van persoonsgegevens in één of meer van de volgende vormen: verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere manier ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen (AVG art. 4). De AVG (zie [paragraaf 1.3](#)) geeft aan wanneer persoonsgegevens verwerkt mogen worden.

1.1.4 Informatiebeveiliging

Informatiebeveiliging is het nemen van maatregelen om informatie goed te beschermen. Dit zorgt ervoor dat informatie betrouwbaar blijft. Dit geldt voor alle gebruikte informatiesystemen (programmatuur, apparatuur, databases, mensen en processen), informatiedragers (papier of digitaal) en persoonsgegevens. Alle systemen en gegevens moeten worden beschermd tegen ongewenste toegang of schade; of dit nu per ongeluk gebeurt of expres (Kennisnet z.d.b).

Informatiebeveiliging richt zich op drie aspecten:

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

(Kennisnet z.d.a).

1.1.5 Bestand

Een bestand is een verzameling persoonsgegevens die op een bepaalde manier is georganiseerd en makkelijk toegankelijk is (AVG art. 4). Dit kan bijvoorbeeld een digitaal bestand zijn, maar ook een archiefkast of een stapel naamkaartjes. Er is ook sprake van de verwerking van persoonsgegevens wanneer deze in een bestand worden opgenomen of bestemd zijn om daarin opgenomen te worden. Losse papieren op een bureau met daarin de namen van personen vormen geen bestand, mits deze niet digitaal opgeslagen zijn (Kennisnet z.d.b).

1.1.6 Autoriteit Persoonsgegevens

De Autoriteit Persoonsgegevens (AP) is de organisatie in Nederland die toezicht houdt op de privacy van mensen. Ze controleert of organisaties zich aan de regels houden van de AVG. Als mensen denken dat hun privacy niet goed wordt beschermd, kunnen ze bij de AP terecht. De AP kan organisaties ook boetes geven als ze de regels niet volgen en geeft advies over hoe persoonsgegevens goed beschermd kunnen worden.

1.2 Reikwijdte

Het Reglement Privacy geldt voor en heeft betrekking op alle medewerkers, leerlingen, ouders/verzorgers, samenwerkingspartners, leveranciers en andere betrokkenen bij VO Veghel. Het reglement geldt voor alle toepassingen die vallen onder de verantwoordelijkheid van VO Veghel. Hieronder valt de gecontroleerde informatie die door de scholen zelf wordt

gemaakt en beheerd. Ook valt hieronder de niet-gecontroleerde informatie waar de school verantwoordelijk voor kan worden gehouden, zoals uitspraken van medewerkers en leerlingen op websites en sociale media. Het reglement is daarnaast van toepassing op alle automatische en systematische verwerkingen van persoonsgegevens waarvoor VO Veghel verantwoordelijk is. Het Reglement Privacy geldt ook voor de niet-automatische verwerking van persoonsgegevens die in een bestand zijn opgeslagen of daarin moeten worden opgenomen.

1.3 AVG

De AVG stelt eisen aan de manier waarop organisaties omgaan met privacygevoelige informatie. Organisaties zijn zelf verantwoordelijk voor de naleving van de regels van de AVG. Het is belangrijk dat organisaties zich bewust zijn van de risico's die gegevensverwerking met zich meebrengt en dat zij transparant communiceren over deze verwerking.

De AVG heeft zes beginselen (ook wel basisprincipes genoemd). Iedereen die persoonsgegevens verwerkt, moet zich aan deze beginselen houden en kunnen aantonen dat hij zich hieraan houdt. Dit is de verantwoordingsplicht (AVG art. 5). De zes beginselen zijn:

1. **Rechtmatigheid, behoorlijkheid en transparantie:** de verwerking van persoonsgegevens is altijd gebaseerd op een van de zes wettelijke grondslagen: toestemming, overeenkomst, wettelijke verplichting, vitaal belang, algemeen belang of gerechtvaardigd belang (zie [paragraaf 1.3.1](#) en [paragraaf 2.1](#)). Daarnaast is de verwerking altijd 'behoorlijk'. Dit betekent dat de verwerking niet nadelig, discriminerend, onverwacht of misleidend mag zijn voor de betrokkenen. Ook is de verwerking transparant: leerlingen, ouders/verzorgers, medewerkers en andere betrokkenen moeten weten welke gegevens VO Veghel verzamelt en wat ermee gebeurt. VO Veghel maakt dit duidelijk in dit Reglement Privacy. Alle betrokkenen hebben het recht om hun gegevens in te zien (zie [paragraaf 2.2](#));
2. **Doelbinding en doelbepaling:** persoonsgegevens worden alleen verwerkt voor doelen die van tevoren duidelijk zijn beschreven en die terecht zijn. Persoonsgegevens worden niet verder verwerkt voor een ander doel of op een manier die niet overeenkomt met het doel (zie [paragraaf 2.3](#));
3. **Dataminimalisatie:** de hoeveelheid en soort persoonsgegevens die verwerkt worden, blijft beperkt. Het verwerken van de persoonsgegevens moet nodig zijn om het doel van de organisatie te bereiken, namelijk het bieden van kwalitatief goed onderwijs. Met andere woorden: de gegevens staan in verhouding tot het doel

(proportionaliteit) en het doel kan niet met minder, alternatieve of andere gegevens worden bereikt (subsidiariteit);

4. **Juistheid:** gegevens zijn juist, wat betekent dat deze actueel zijn. Veranderingen in gegevens worden zo snel mogelijk verwerkt (zie [paragraaf 2.4](#));
5. **Opslagbeperking:** gegevens worden bewaard zolang dat nodig is en daarna verwijderd (zie [paragraaf 2.5](#));
6. **Vertrouwelijkheid en integriteit:** gegevens worden goed beveiligd (zie [paragraaf 2.6](#)).

In [hoofdstuk 2](#) staat beschreven hoe VO Veghel ervoor zorgt dat zij aan de beginselen voldoet.

1.3.1 Grondslagen

Er zijn zes wettelijke grondslagen op basis waarvan persoonsgegevens verwerkt mogen worden (Autoriteit Persoonsgegevens z.d.b):

1. **Toestemming:** de persoon van wie gegevens worden verwerkt heeft toestemming gegeven voor de verwerking. Zie het Protocol Toestemming Verwerking Persoonsgegevens voor de eisen waaraan toestemming moet voldoen om geldig te zijn;
2. **Overeenkomst:** het verwerken van gegevens is nodig om een overeenkomst uit te voeren. Op deze grondslag mag gegevensverwerking gebaseerd worden als een overeenkomst alleen kan worden uitgevoerd door persoonsgegevens te verwerken;
3. **Wettelijke verplichting:** het verwerken van gegevens is nodig omdat dit wettelijk verplicht is. Denk bijvoorbeeld aan het delen van salarisinformatie van medewerkers met de Belastingdienst voor de uitvoering van de belastingwetgeving of het delen van gegevens over de onderwijsprogramma's van leerlingen met Dienst Uitvoering Onderwijs (DUO);
4. **Vitaal belang:** het verwerken van gegevens is nodig om vitale belangen te beschermen. Een vitaal belang is een belang dat onmisbaar is voor iemands leven of gezondheid, terwijl een persoon niet om toestemming kan worden gevraagd om zijn gegevens te verwerken. Dit is bijvoorbeeld het geval als een persoon buiten bewustzijn is en zijn leven in gevaar is;
5. **Algemeen belang:** het verwerken van gegevens is nodig om een taak van algemeen belang uit te voeren of om openbaar gezag uit te oefenen. Deze grondslag is voornamelijk van toepassing binnen overheidsinstanties zoals gemeenten;

6. **Gerechtvaardigd belang:** het verwerken van gegevens is nodig om gerechtvaardigde belangen (zie 6a) van personen te beschermen. Er moet dan aan drie voorwaarden worden voldaan:
- a. Er is werkelijk sprake van een gerechtvaardigd belang. Een belang is gerechtvaardigd als het in het recht is beschermd, zoals de zorgplicht voor werknemers;
 - b. De verwerking is nodig om het belang te beschermen. Dit betekent dat de verwerking van de gegevens in verhouding staat tot de inbreuk op de privacy van de betrokkenen. Dit is het uitgangspunt van *proportionaliteit*. Daarnaast mag het doel niet op een andere, minder ingrijpende manier bereikt kunnen worden. Dit is het uitgangspunt van *subsidiariteit*. Pas wanneer sprake is van proportionaliteit en subsidiariteit, kan een verwerking werkelijk nodig zijn;
 - c. De organisatie heeft haar eigen belangen afgewogen tegen die van de betrokkenen. Bij de afweging worden vier zaken onderzocht:
 - i. De gevolgen voor de betrokkenen;
 - ii. De ernst van de inbreuk op de privacy van betrokkenen;
 - iii. De (aanvullende) maatregelen die worden genomen om ongewenste gevolgen voor betrokkenen te voorkomen of beperken;
 - iv. Of de betrokkenen de verwerking min of meer kunnen verwachten.
- Alleen wanneer de belangen van VO Veghel zwaarder wegen dan de belangen van de betrokkenen, mogen persoonsgegevens worden verwerkt op basis van de grondslag 'gerechtvaardigd belang'. Deze belangenafweging wordt gemaakt middels een *Legitimate Interest Assessment* (LIA).

2 Werkwijze VO Veghel

In dit hoofdstuk staat beschreven hoe VO Veghel ervoor zorgt dat ze voldoet aan de beginselen van de AVG met betrekking tot de verwerking van persoonsgegevens.

2.1 Grondslagen en soorten gegevens

VO Veghel verwerkt *reguliere* persoonsgegevens vooral op basis van de grondslagen 'toestemming', 'wettelijke verplichting' en 'gerechtvaardigd belang'. Reguliere persoonsgegevens die verwerkt worden, zijn:

1. Medewerkers inclusief vrijwilligers en stagiaires: naam-, adres- en contactgegevens, BSN, geboortedatum en -plaats, rekeningnummer, identiteitsbewijs, VOG en contactgegevens in geval van nood;
2. Medewerkers inclusief vrijwilligers (exclusief stagiaires): alle bovengenoemde gegevens, aangevuld met bevoegdheden en scholingsbewijzen, nationaliteit, loonbelastingverklaring, onderwijsjaren en dienstjaren, laatste salarisstrook, loonbelastingverklaring en hoofd- en nevenbetrekkingen en vanaf welk IP-adres op welke dag en welke tijd een medewerker inlogt;
3. Leerlingen: zie het aanvraagformulier ([bijlage 1](#)) en het overdrachtsformulier ([bijlage 2](#)). Daarnaast wordt in het leerlingadministratiesysteem, indien nodig, de volgende informatie verzameld: schoolresultaten, kenmerken (waaronder leerstoornissen en beperkingen), psychologische onderzoeken, ondersteuningsbehoeften, hulpmiddelen, aan- en afwezigheid, lesnotities (van bijzonderheden tijdens de les), incidenten en maatregelen, contact met ouders/verzorgers, externe contactpersonen (van zorginstanties) en toestemmingsverklaringen. Ook is bekend vanaf welk IP-adres op welke dag en welke tijd een leerling inlogt;
4. Ouders/verzorgers: zie aanmeldformulier ([bijlage 1](#));
5. Overige betrokkenen: naam- en contactgegevens;
6. Alle betrokkenen: overige gegevens, indien nodig en afhankelijk van de situatie.

Daarnaast verwerkt VO Veghel *bijzondere* persoonsgegevens op basis van de grondslagen 'wettelijke verplichting' of 'uitdrukkelijke toestemming' (Autoriteit Persoonsgegevens z.d.b).

Bijzondere gegevens die verwerkt worden, zijn:

1. Camerabeelden van alle betrokkenen die zich op het schoolterrein of in het schoolgebouw bevinden (zie Protocol Cameratoezicht en Reglement Cameratoezicht);

2. Medische gegevens van leerlingen indien noodzakelijk om de veiligheid en gezondheid te waarborgen en mits toestemming is verkregen van de leerling en/of zijn wettelijk vertegenwoordiger;
3. Aantekeningen van gesprekken met (gevoelige) persoonlijke informatie;
4. Gegevens over het welzijn (via een enquête);
5. Overige informatie, afhankelijk van de situatie.

2.2 Rechten en klachten

Betrokkenen van wie persoonsgegevens worden verwerkt door VO Veghel of een partner van VO Veghel hebben zes privacyrechten, namelijk: het recht op inzage, correctie, verwijdering, beperking, overdraagbaarheid en bezwaar. In het Beleid Rechten Betrokkenen wordt toegelicht wat deze rechten inhouden en hoe betrokkenen gebruik kunnen maken van hun rechten. Wanneer u ontevreden bent over de manier waarop er met uw gegevens wordt omgegaan, dan kunt u een klacht indienen. U dient uw klacht in bij de betreffende medewerker of via privacy@voveghel.nl. Heeft u de wens om een formele klacht in te dienen, dan kan dat volgens de klachtenprocedure van OMO.

2.3 Doelen

Persoonsgegevens worden alleen verzameld wanneer deze noodzakelijk zijn voor het overkoepelende doel van VO Veghel om goed onderwijs te kunnen verzorgen. Om dit overkoepelende doel te bereiken, is het niet alleen noodzakelijk dat onderwijsresultaten aan leerlingen kunnen worden gekoppeld in het leerlingadministratiesysteem, maar bijvoorbeeld ook dat contact met leerlingen en ouders/verzorgers kan plaatsvinden, dat salaris kan worden uitbetaald aan medewerkers en dat contracten kunnen worden afgesloten met leveranciers.

2.4 Juistheid

Om ervoor te zorgen dat gegevens juist en actueel blijven, hanteert VO Veghel verschillende werkwijzen. Deze staan hieronder beschreven.

2.4.1 Regelmatige controle en actualisatie van gegevens

Leerlingen en ouders/verzorgers controleren of hun gegevens kloppen in het leerlingadministratiesysteem. Veranderingen voeren zij zelf door of geven zij zo snel mogelijk door aan de teamleider (zoals beschreven in Beleid Rechten Betrokkenen). Als gegevens ontbreken, worden ouders/verzorgers gebeld door een medewerker om de gegevens aan te vullen.

Medewerkers controleren of hun gegevens kloppen in het personeelsinformatiesysteem. Als de gegevens niet (meer) kloppen, passen zij dit zelf zo snel mogelijk aan. Ook leveranciers en andere externe partijen geven wijzigingen zo snel mogelijk door. Contracten met externe partijen worden beheerd in de contractmodule van het personeelsinformatiesysteem. Het personeelsinformatiesysteem geeft automatisch een seintje om te controleren of de gegevens in contracten nog kloppen. Bij stilzwijgende verlenging controleert de contractverantwoordelijke periodiek of de gegevens nog kloppen.

2.4.2 Geautomatiseerde systemen

Het personeelsinformatiesysteem verwijdert automatisch gegevens die de bewaartermijn hebben bereikt. Daarnaast zijn verplichte velden ingesteld om ervoor te zorgen dat belangrijke gegevens, zoals geboortedata en adressen, altijd worden ingevuld.

2.5 Bewaartermijnen

Om gegevens niet langer te bewaren dan nodig is (beginsel 'dataminimalisatie') hanteert VO Veghel bewaartermijnen die wettelijk en door vereniging Ons Middelbaar Onderwijs (OMO) zijn bepaald. Meer informatie hierover is te vinden in het Protocol Bewaren en Vernietigen.

2.6 Beveiliging van gegevens

2.6.1 Functionarissen en beleid

De Privacy Officer en de Functionaris Informatiebeveiliging van VO Veghel maken het beleid op het gebied van informatiebeveiliging en privacy (IBP) en zorgen ervoor dat dit actueel blijft. De awarenesscoördinator van VO Veghel zorgt ervoor dat betrokkenen op de hoogte zijn van dit beleid. Binnen OMO zijn enkele functionarissen aanwezig die kaders en ondersteuning bieden waar nodig, waaronder de Privacy Officer (PO), de Functionaris Gegevensbescherming (FG) en de Security Officer (SO). De PO maakt het kader voor het privacybeleid voor alle OMO-scholen en ondersteunt bij het uitvoeren van risicoanalyses op het gebied van privacy. De FG ondersteunt bij datalekken en doet zo nodig melding bij de Autoriteit Persoonsgegevens. De SO maakt het kader voor het informatiebeveiligingsbeleid voor alle OMO-scholen en biedt ondersteuning bij de implementatie en uitvoer daarvan.

VO Veghel betreft de PO en FG tijdig bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens, bijvoorbeeld door advies te vragen bij iedere DPIA en bij het opstellen van bewustwordingsprogramma's op het gebied van IBP. De PO en FG zijn telefonisch bereikbaar en via de mail (respectievelijk po@omo.nl en fg@omo.nl).

2.6.2 Digitale en fysieke beveiliging

Gegevens worden beveiligd middels vele verschillende digitale en fysieke beveiligingsmaatregelen, waaronder back-ups, een wachtwoordbeleid en sleutels of tags met verschillende toegangsniveaus (zie Beleid Informatiebeveiliging). Dit is ook het geval wanneer gegevens gedeeld worden. Binnen VO Veghel worden persoonsgegevens binnen de digitaal en/of fysiek beveiligde omgeving gedeeld. Buiten VO Veghel worden persoonsgegevens gedeeld via een beveiligde tool van OMO. Sommige gegevens worden door externe partijen verwerkt onder verantwoordelijkheid van VO Veghel. Met deze partijen is een verwerkersovereenkomst afgesloten waarin afspraken zijn opgenomen over de manier waarop de gegevens verwerkt en beveiligd worden. Gegevens worden nooit buiten de Europese Economische Ruimte (EER) gedeeld (zie Beleid Privacy).

Alle apparatuur is beveiligd met een TPM 2.0 chip en alle apparatuur is voorzien van Bitlocker. Apparatuur kan op afstand gewist worden. Alle apparatuur is gekoppeld met Intune waardoor je er niet op kunt inloggen met aan ander account (alleen een VO Veghel-mailadres met bijbehorend wachtwoord). Mobiele datadragers die niet standaard beveiligd zijn, zoals een usb-stick of externe harde schijf, moeten voorzien zijn van Bitlocker; dit is de verantwoordelijkheid van de gebruiker.

2.6.3 Beperking van toegang en verantwoordelijkheid

Alleen personen in relevante functies hebben toegang tot persoonsgegevens en zijn verantwoordelijk voor het bijhouden ervan. Op deze manier bestaat er minder kans op fouten of onzorgvuldige verwerking.

2.6.4 Risicoclassificaties en risicoanalyses

Binnen VO Veghel wordt de beveiliging van gegevens gebaseerd op risicoclassificaties en risicoanalyses. Dit gebeurt volgens het Beleid Privacy en het Beleid Informatiebeveiliging. Op basis van vastgestelde risico's worden zoveel mogelijk maatregelen genomen om de risico's te beperken. Dit gebeurt voordat een nieuwe toepassing of werkwijze wordt geïmplementeerd.

2.6.5 Beveiligingsincidenten en datalekken melden en registreren

Ondanks alle beveiligingsmaatregelen kunnen er beveiligingsincidenten en datalekken plaatsvinden. Bij een beveiligingsincident is *informatie* verloren of op een verkeerde manier verwerkt. Dit kunnen persoonsgegevens zijn, maar dat hoeft niet. Bij een beveiligingsincident komt de vertrouwelijkheid, integriteit of beschikbaarheid van informatie of informatieverwerkende systemen in gevaar; denk aan een besmetting met een virus of een mail met gevoelige informatie die buiten de beveiligde omgeving is verzonden. Een datalek is

een beveiligingsincident waarbij (mogelijk) *persoonsgegevens* zijn verloren of op een verkeerde manier zijn verwerkt.

Beveiligingsincidenten en datalekken worden door medewerkers gemeld via een formulier op de startpagina in Teams (zie Protocol Beveiligingsincidenten en Datalekken). Overige betrokkenen kunnen beveiligingsincidenten en datalekken melden bij een medewerker of via privacy@voveghel.nl. Meldingen worden afgehandeld door de Privacy Officer van VO Veghel en zo nodig door de PO en FG van OMO. De FG van OMO meldt datalekken bij de Autoriteit Persoonsgegevens als dit nodig is. Maatregelen worden zo snel mogelijk genomen om negatieve gevolgen te beperken. In het geval van grote crises, zoals bijvoorbeeld een hack waardoor het onderwijsproces (gedeeltelijk) stil komt te liggen, wordt de crisis afgehandeld door het crisismanagementteam volgens het Cybersecuritycrisisplan van VO Veghel.

Gemelde beveiligingsincidenten en datalekken worden geregistreerd en vastgelegd in een jaarverslag. Tijdens het opstellen van dit jaarverslag wordt de status en voortgang van de informatiebeveiliging binnen VO Veghel geëvalueerd en worden doelen opgesteld om deze verder te verbeteren. Het jaarverslag is in te zien op aanvraag via privacy@voveghel.nl

3 Evaluatie

Het Reglement Privacy wordt eens per twee jaar geëvalueerd. De evaluatie wordt uitgevoerd door de Privacy Officer. Tijdens de evaluatie worden antwoorden gegeven op de volgende vragen:

1. Doen we de goede dingen?
2. Doen we de dingen goed?
3. Hoe weten we dat?
4. Vinden anderen dat ook?
5. Wat doen we vervolgens?

De antwoorden op bovenstaande vragen worden gebaseerd op de volgende bronnen:

- Nieuwe of gewijzigde wet- en regelgeving;
- Het jaarverslag waarin informatie is opgenomen over het verwerkingsregister, de uitgevoerde risicoanalyses, het aantal en de soorten gemelde beveiligingsincidenten en datalekken, verzoeken van betrokkenen, klachten met betrekking tot IBP en verbeterplannen;
- De evaluaties van genoemde beleidsplannen en protocollen.

Tips van betrokkenen zijn altijd welkom. U kunt deze mailen naar privacy@voveghel.nl.

Indien nodig worden aanpassingen in het reglement gedaan door de Privacy Officer. De aanpassingen worden uitgezet en gecommuniceerd binnen VO Veghel door de awarenesscoördinator.

Bronnen

Autoriteit Persoonsgegevens (z.d.a) Wat zijn persoonsgegevens?

[Wat zijn persoonsgegevens? | Autoriteit Persoonsgegevens](#)

Autoriteit Persoonsgegevens (z.d.b). Grondslagen AVG uitgelegd.

[Grondslagen AVG uitgelegd | Autoriteit Persoonsgegevens](#)

Bijlagen

Bijlage 1 Gegevens aanmeldformulier

1. Persoonlijke gegevens en adresgegevens

Roepnaam, geslacht, officiële voornamen, roepnaam, achternaam, geboortedatum, geboorteplaats, geboortegemeente, geboorteland, nationaliteit, evt. tweede nationaliteit, datum in Nederland (indien niet in Nederland geboren), onderwijs in Nederland sinds, telefoonnummer leerling, mailadres leerling, straat, huisnummer, postcode, woonplaats, gemeente, BSN.

2. Aanmelding voor welk leerjaar en welke schoolsoort

3. Aanmelding andere school

Is de leerling ook aangemeld bij een andere school? Zo ja, naam en plaats van deze school.

4. Vrije tijd

Hobby's.

5. Toekomstige klasgenoten

Bij welke leerlingen (maximaal twee) wil uw kind graag in de klas zitten?

6. Begeleiding en ondersteuning

- a. Heeft de leerling in de basisschoolperiode extra begeleiding ontvangen en vermoedt u dat dit gecontinueerd moet worden? Zo ja, toelichting.
- b. Is er sprake van: leerproblemen (dyslexie, dyscalculie e.d.), sociaal-emotionele problematiek (ADD, ADHD, ASS e.d.), vermoedens hoogbegaafdheid, specifieke diagnose, onderliggend verslag aanwezig en wordt dit overhandigd? Toelichting.
- c. Is er sprake van medische problematiek of ziekte waar school van op de hoogte moet zijn? Onderliggend verslag aanwezig en wordt dit overhandigd? Toelichting.

7. School van herkomst

- a. Naam, adres, postcode en plaats, telefoonnummer.
- b. Is de leerling gedoubleerd? Zo ja, in welk leerjaar?
- c. Advies huidige school. Ouders/verzorgers hiermee eens?

8. Bijzondere omstandigheden

- a. Zijn er bijzondere familieomstandigheden (bv. ouders/verzorgers gescheiden/overleden, woonsituatie)?

- b. Zijn beide ouders/verzorgers belast met gezag? Zo nee, wie heeft gezag?
Co-ouderschap?
- c. Wie heeft zorgplicht?
- d. Andere ouder akkoord met aanmelding?
- e. Willen beide ouders per post/e-mail op de hoogte blijven?
- f. Zitten er al kinderen op de school? Zo ja, naam/namen en klas
- g. Hebben er kinderen op de school gezeten? Zo ja, naam/namen

9. Gegevens ouder(s)/verzorger(s)

Voorletter(s), achternaam, relatie tot leerling (vader/moeder/verzorger/anders, namelijk), nationaliteit, geboorteland (i.v.m. taalontwikkeling kind), e-mailadres, telefoon + geheim, adres en IBAN en tenaamstelling.

Bijlage 2 Gegevens overdrachtsformulier

1. Huidige school

- a. Naam
- b. Directeur
- c. Adres (straat, huisnummer, postcode, plaats, gemeente, postadres)
- d. Communicatiegegevens (telefoon en e-mailadres)

2. Leerling

- a. Voornamen, voorletters, achternaam, roepnaam, geboortedatum, geslacht, adres + geheim (straat, huisnummer, postcode, plaats, gemeente, GBA-code, land), BSN, is sprake van een niet-Nederlandse culturele achtergrond.
- b. Leerling-id, datum inschrijving vorige school, datum uitschrijving vorige school.
- c. Verzorgers aansprakelijk.

3. Ouder(s)/verzorger(s)

- a. Voorletters, achternaam, geslacht, relatie tot kind, wettelijk vertegenwoordiger, adres geheim, woonadres (straat, huisnummer, postcode, plaats, gemeente, GBA-code, land).
- b. Communicatiegegevens: telefoon, e-mail.

4. Overstapadvies

Voorlopig en definitief schooladvies.

5. Leerlingrapport doorstroomtoets

Toetssoort, omschrijving, afnamedatum, ontheffing, standaardscore, toetsadvies, referentieniveau rekenen, taalverzorging en lezen.

6. Huisarts

Naam, adres (straat, huisnummer, postcode, plaats, gemeente, GBA-code, land), telefoonnummer.

7. Verzuim

Dagdelen geoorloofd en dagdelen ongeoorloofd verzuim.