Privacy en veiligheid
deel A: leerlingen en ouders

#Jijdoetertoe

VCO HIERDEN HARDERWIJK

Vertrouwelijkheid: openbaar

Auteur: afdeling B&O

Versie: 2.1

Februari 2026

Inhoud

Inhoud	3
Inleiding	4
Visie en kernwaarden van VCO	5
Wat is de AVG?	6
Autoriteit persoonsgegevens	7
AVG	8
Bewaren leerling gegevens	9
Cameratoezicht	11
ECK-id	16
Functionaris gegevensbescherming	17
Gedragscode AVG voor leerlingen	19
Grondslagen VCO	21
Informatiebeveiliging en privacy (IBP)	29
Privacy statement leerlingen	30
Rechten van betrokkenen	36
Recht op vergetelheid	46

Inleiding

Stichting voor Christelijk Onderwijs Harderwijk-Hierden (VCO), heeft een duidelijke koers. De VCO-Koers heeft de titel 'Vastberaden Vooruit' meegekregen, om te duiden dat we krachtig voor onze Koers stáán en gáán. Als onderwijsorganisatie hebben we ons te verhouden tot een dynamische en veeleisende samenleving. Onze VCO-Koers 'Vastberaden Vooruit' helpt ons om dicht bij onszelf en onze weloverwogen bedoelingen te blijven. Onze koers wordt nader omschreven in ons koersplan, te vinden op de website. Maar ook in dit digitaal veiligheidsplan vertaalt het zich.

Met 12 scholen en een grote gemeenschap van leerlingen, medewerkers en ouders, zet VCO zich in om een veilige leer- en werkomgeving te bieden die aansluit bij haar christelijke kernwaarden.

Digitale veiligheid speelt hierin een cruciale rol. Het beschermen van persoonsgegevens en het waarborgen van een veilige digitale infrastructuur zijn essentieel om de privacy van leerlingen, ouders en medewerkers te waarborgen en de continuïteit van onderwijs te garanderen.
Dit digitale veiligheidsplan geeft inzicht in de maatregelen en richtlijnen die VCO hanteert om digitale risico's te minimaliseren. Het plan is opgesteld in lijn met de geldende wet- en regelgeving en sluit aan bij de missie en visie van VCO. Hiermee onderstreept VCO haar verantwoordelijkheid en toewijding om een veilige en vertrouwde omgeving te creëren, zowel fysiek als digitaal.

In dit plan beschrijft VCO de doelstellingen maar geven wij ook onze missie en visie weer. Immers dat geeft duidelijkheid aan eenieder waar VCO samen naar toe werkt. Het helpt VCO bij het nemen van beslissingen en het geeft vertrouwen dat VCO weet waar wij mee bezig zijn. Het digitaal veiligheidsplan wordt jaarlijks gecontroleerd en waar nodig aangevuld en aangepast.*

Mocht u naar aanleiding van dit plan vragen hebben, neem dan contact op met onze privacy officer, te bereiken via avg@stichtingvco.nl

**De versiegeschiedenis en goedkeuring door GMR en CvB zijn op te vragen via de privacy officer.*

Visie en kernwaarden van VCO

Missie:
“Leerlingen laten groeien, in kennis en vaardigheden en als mens”

Motto en kernwaarden:
“Wij geloven in goed onderwijs voor elk kind!”

“Wij geloven in goed onderwijs voor elk kind!” Ons motto verwoordt een positieve invulling aan opdracht en doel zoals deze in de stichtingsstatuten zijn omschreven waarbij “Opvoeding en onderwijs niet gescheiden kunnen worden.” Wij laten ons inspireren en leiden door het Liefdegebod uit Korintiërs 13. Het geeft een vooruitblik aan Gods Koninkrijk en reikt ons vanuit onze identiteit drie kernwaarden aan: geloof, hoop en liefde.

Zorgen voor fysieke veiligheid is niet een op zichzelf staande opdracht. Een veilige omgeving is een belangrijke voorwaarde voor kinderen om zich goed te kunnen ontwikkelen. VCO is wettelijk verplicht om de fysieke veiligheid van leerlingen te waarborgen. Naast deze fysieke veiligheid bieden wij alle kinderen goed onderwijs en we stellen onze kernwaarden centraal. De kernwaarden geven aan waarvoor we staan, wie we willen zijn en wat alle medewerkers van VCO verbindt. Wij streven ernaar dat de kernwaarden telkens zichtbaar zijn in ons handelen.

Geloof
Wij geloven en handelen vanuit christelijke waarden. Wij leven ons geloof en willen een goed voorbeeld zijn. Wij benaderen elkaar met respect en vertrouwen. Wij geloven in goed onderwijs voor ieder kind

Hoop
Wij zijn positief gericht op de toekomst. Wij zetten in op goed onderwijs. Wij leren met en van elkaar. Wij maken gebruik van en ontwikkelen elkaars talenten

Liefde
Wij zien het kind. Wij zien het kind in relatie met die ander. Wij zien het kind in relatie tot de aarde en zijn omgeving. Wij werken samen. Wij nemen verantwoordelijkheid.

Wat is de AVG?

AVG staat voor Algemene Verordening Gegevensbescherming. Het is een Europese wetgeving die van kracht is sinds 25 mei 2018. De AVG regelt hoe organisaties in de Europese Unie (EU) moeten omgaan met persoonlijke gegevens. Het doel ervan is om de privacy van individuen te beschermen door strikte regels op te stellen voor het verzamelen, verwerken en bewaren van persoonlijke gegevens.
De AVG legt verplichtingen op aan organisaties, zoals het verkrijgen van expliciete toestemming van individuen voordat hun gegevens worden verzameld, het beschermen van deze gegevens tegen misbruik en ongeautoriseerde toegang, en het rapporteren van datalekken aan de relevante autoriteiten en betrokkenen.
In de AVG staan de volgende 6 grondslagen voor het verwerken van persoonsgegevens:

1. Toestemming van de betrokkene (bijvoorbeeld de ouder):*Voorbeeld: Een basisschool vraagt ouders om toestemming om foto's van hun kinderen te gebruiken voor de schoolwebsite of voor publicaties in de schoolkrant.*
2. Uitvoering van een overeenkomst (zoals het onderwijscontract):
   Voorbeeld: De basisschool verwerkt persoonsgegevens van leerlingen om onderwijs te kunnen bieden, zoals het bijhouden van aanwezigheid, cijferregistratie en communicatie met ouders over de voortgang van hun kinderen.
3. Wettelijke verplichting:
   Voorbeeld: De school verwerkt persoonsgegevens van leerlingen om te voldoen aan rapportageverplichtingen aan de onderwijsinspectie.
4. Vitaal belang van de betrokkene:
   Voorbeeld: In geval van een medische noodsituatie op school verwerkt de school mogelijk persoonsgegevens van een leerling om medische hulp te verlenen in het belang van het welzijn en de veiligheid van de leerling.
5. Taak van algemeen belang of uitoefening van het openbaar gezag:

   Voorbeeld: De school verwerkt persoonsgegevens van leerlingen om te voldoen aan onderwijsdoelstellingen en de educatieve verantwoordelijkheden die door de overheid zijn vastgesteld, zoals onderwijsstatistieken en de verplichte deelname aan onderwijs.
6. Gerechtvaardigd belang van de verwerkingsverantwoordelijke (bijvoorbeeld de school):
   Voorbeeld: De school verwerkt persoonsgegevens van ouders en leerlingen voor communicatiedoeleinden met betrekking tot schoolactiviteiten, zoals uitnodigingen voor ouderavonden of informatie over buitenschoolse activiteiten.

Door deze grondslagen te respecteren en toe te passen, zorgt de basisschool ervoor dat zij voldoet aan de wettelijke eisen van de AVG bij het verwerken van persoonsgegevens van leerlingen, ouders en personeel.

Autoriteit persoonsgegevens

U heeft een functionaris voor de gegevensbescherming (FG) voor uw organisatie Stichting voor christelijk Onderwijs Harderwijk- Hierden (VCO).

Het aan u toegekende FG-nummer is FG004270.

Meer informatie over de FG vindt u op https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/functionaris-voor-de-gegevensbescherming. Zoekt u aanvullende informatie? Dan kunt u hiervoor terecht bij het Nederlands Genootschap voor de Functionaris voor de Gegevensbescherming, het NGFG. Meer informatie over het NGFG vindt u op www.ngfg.nl.

Graag geven wij u nog aanvullende informatie over de positie van de FG binnen VCO:

- VCO moet de FG genoeg middelen ter beschikking stellen om zijn taken goed te vervullen.
- VCO mag de FG geen instructies geven over het uitvoeren van de FG-taken; de FG voert zijn taken en verplichtingen onafhankelijk uit.
- De FG mag naast zijn FG-taken eventueel andere taken of functies vervullen, maar er mag geen sprake zijn van belangenverstrengeling.
- VCO is verplicht de contactgegevens van de FG openbaar te maken.

AUTORITEIT
PERSOONSGEGEVENS

FG@autoriteitpersoonsgegevens.nl
T 070 8888 500 - F 070 8888 501
Prins Clauslaan 60, 2595 AJ Den Haag
Postbus 93374, 2509 AJ Den Haag
autoriteitpersoonsgegevens.nl

AVG

Algemene verordening gegevensbescherming (AVG)

Met het oog op onze voortdurende inzet voor transparantie, integriteit en de bescherming van persoonsgegevens heeft onze school de Algemene Verordening Gegevensbescherming (AVG) hoog in het vaandel staan. De AVG, die sinds mei 2018 van kracht is, vormt de hoeksteen van ons streven naar een zorgvuldige omgang met persoonsgegevens binnen onze school.

Achtergrond van de AVG

De AVG is een Europese privacywet. Deze wet geeft leerlingen, ouders en medewerkers meer rechten en geeft organisaties meer verantwoordelijkheid om zorgvuldig met (digitale) persoonsgegevens om te gaan.

Principes van de AVG binnen onze school

a) *Wettelijke grondslag:* Wij verwerken persoonsgegevens alleen op basis van de wettelijke grondslagen, waaronder toestemming, contractuele verplichtingen, wettelijke verplichtingen, vitale belangen, publieke taak of gerechtvaardigde belangen.
b) *Transparantie:* Wij informeren alle betrokkenen op heldere wijze over de doeleinden van gegevensverwerking, de categorieën van verzamelde gegevens en de rechten van betrokkenen.
c) *Rechten van betrokkenen:* Wij respecteren en faciliteren de rechten van betrokkenen zoals het recht op inzage, correctie, verwijdering, beperking van verwerking en dataportabiliteit.
d) *Data minimalisatie:* Wij verzamelen alleen persoonsgegevens die strikt noodzakelijk zijn voor de specifieke doeleinden en beperken de bewaartermijnen tot wat nodig is.

Maatregelen en procedures binnen onze school

a) *Beveiligingsmaatregelen:* Wij implementeren technische en organisatorische maatregelen om persoonsgegevens te beschermen tegen ongeoorloofde toegang, verlies, vernietiging of wijziging.
b) *Data Protection Impact Assessments (DPIA):* Waar nodig voeren wij DPIA's uit om de potentiële impact van gegevensverwerking op de privacy van betrokkenen te beoordelen.
c) *Functionaris Gegevensbescherming (FG) en Privacy Officer:* Onze school heeft een aangewezen Functionaris voor Gegevensbescherming en Privacy Officer om toezicht te houden op de naleving van de AVG en als aanspreekpunt voor vragen over gegevensbescherming.

Op de site van onze stichting kunt u verder documenten vinden rondom de verwerking en beveiliging van uw persoonsgegevens: *www.stichtingvco.nl/informatie/Privacy*

Bewaren leerling gegevens

Alle scholen van de stichting VCO Harderwijk-Hierden (VCO) bewaren gegevens over ingeschreven leerlingen in een leerlingdossier, bijvoorbeeld leerresultaten en aanwezigheid. Ouder(s) en/of verzorger(s) en de school mogen deze gegevens inzien. In speciale gevallen mogen anderen dat ook. Bijvoorbeeld in een noodsituatie of bij een vermoeden van kindermishandeling. Hieronder beschrijven wij als VCO wat wij verstaan onder leerling gegevens, hoe wij deze bewaren en hoe lang we dit mogen.
VCO mag de gegevens niet langer bewaren dan noodzakelijk is.

Leerling gegevens

Alle scholen van de VCO houden van elke leerling een leerling dossier bij.
Daarin bewaart de school:

- gegevens over inschrijving en uitschrijving;
- gegevens over afwezigheid;
- adresgegevens;

Ook de volgende gegevens mag de school bewaren:

- gegevens over de vorderingen en de resultaten van uw kind;
- gegevens over de gezondheid die nodig zijn voor speciale begeleiding of voorzieningen;
- gegevens over de ondersteuningsbehoefte, als uw kind die heeft.

Bewaren leerling gegevens

De school mag de meeste gegevens nog 2 jaar bewaren, nadat uw kind van school is gegaan. De school moet langer bewaren:

- gegevens over verzuim en in- en uitschrijving (5 jaar na vertrek);
- gegevens over een leerling die naar een school voor speciaal onderwijs is doorverwezen (3 jaar na vertrek);
- adresgegevens van (oud-)leerlingen mag de school bewaren voor het organiseren van reünies.

Inzage en correctie leerling gegevens

Ouder(s) en/of verzorger(s) hebben het recht om de gegevens over hun kind(eren) in te zien (inzagerecht). Zij maken hiervoor een afspraak met de school. Terwijl zij de gegevens inzien, blijft iemand van de school aanwezig. Ouder(s) en/of verzorger(s) hebben ook correctierecht. Zij kunnen de school vragen verkeerde gegevens (gemotiveerd) in het leerling dossier van de leerling te verbeteren of te verwijderen. Het dossier blijft op school, er kan wel gevraagd worden om een kopie.
Is er geen ouderlijk gezag meer, bijvoorbeeld na een echtscheiding? Dan is er geen recht op een kopie (inzagerecht). Wel moet de school inzage geven in de leerling gegevens over de leerling. Dit

staat in het Burgerlijk Wetboek. De ouder(s) en/of verzorger(s) moet dan zelf de directeur van de school om deze informatie vragen.

Inzage leerling gegevens door anderen

Soms is de school verplicht om informatie over de leerling aan bepaalde deskundigen te geven. Bijvoorbeeld:

- medewerkers in het voortgezet onderwijs (vo) of het speciaal basisonderwijs (sbo): wanneer uw kind de basisschool verlaat;
- hulpverleners: bijvoorbeeld bij noodsituaties of vermoedens van kindermishandeling;
- Inspectie van het Onderwijs (IvhO).

In andere gevallen moeten ouder(s) en/of verzorger(s) eerst toestemming geven (zie formulier toestemming uitwisseling leerling gegevens).

Cameratoezicht

Dit reglement heeft betrekking op alle locaties van Stichting VCO waar toezicht door middel van cameratoezicht wordt toegepast door middel van camerasystemen. Het reglement beschrijft de taken, verantwoordelijkheden en de procedures met betrekking tot het cameratoezicht. Het doel is het zorgvuldig gebruik van het camerasysteem en de bescherming van de privacy van leerlingen, medewerkers en bezoekers waarborgen.

Artikel 1 – Begripsbepalingen

In dit reglement wordt verstaan onder:

- Cameratoezicht: toezicht met behulp van camera's, waardoor er sprake is van verwerking van persoonsgegevens als bedoeld in de Algemene Verordening Gegevensbescherming (AVG)).
- Serverruimte: de van een toegangscontrolesysteem voorziene ruimte, waar de server of opnameapparatuur staat waarop de opgenomen camerabeelden geregistreerd staan.
- Camerasysteem: het geheel van camera's, monitoren, opnameapparatuur, verbindingskasten, verbindingen en bevestigen waarmee het cameratoezicht wordt uitgevoerd.
- Flexruimte: een centraal gesitueerde, van een toegangscontrolesysteem voorziene ruimte, waarin de camerabeelden - van alle locaties - centraal live kunnen worden bekeken en/of waar ook de mogelijkheid bestaat om opgenomen camerabeelden terug te kijken.
- Camerabeeld: het door het cameratoezicht verkregen camerabeeld.
- Beheerder: de door het college van bestuur aangewezen Privacy officier van VCO, die verantwoordelijk is voor de inrichting, het beheer en toezicht op het cameratoezicht.
- Locatiebeheerder: een door de beheerder als zodanig aangewezen persoon die belast is met het cameratoezicht op één of meerdere locaties van de onderwijsinstelling.
- Technisch beheerder: de functionaris, die onder verantwoordelijkheid van de beheerder, is belast met het technisch beheer van het camerasysteem (Serve IT bv).
- Bevoegde medewerker: een door de beheerder [in geval van cameratoezicht op meerdere locaties: de locatiebeheerder] als zodanig aangewezen persoon die betrokken is bij de uitvoering van het cameratoezicht (hoofd technische dienst VCO, medewerkers B&O).
- Incident: een waargenomen ongewenst en/of strafbaar feit, ongeval of andere gebeurtenis die vraagt om handhaving, onderzoek en/of strafrechtelijke vervolging.

Artikel 2 –Werkingssfeer en doelstellingen cameratoezicht

- Dit reglement is van toepassing op leerlingen en/of hun wettelijk vertegenwoordiger, medewerkers en bezoekers die zich bevinden rondom de gebouwen of op de terreinen van Stichting VCO.
- Het inzetten van cameratoezicht, en het gebruik van de camerabeelden, is alleen toegestaan voor:

a) de bescherming van de veiligheid en gezondheid van leerlingen, medewerkers en bezoekers;

b) de beveiliging van de toegang tot gebouwen en terreinen, waaronder mede is begrepen het weren van ongewenste bezoekers;

c) de bewaking van zaken die op terreinen van VCO bevinden;

d) het vastleggen van incidenten.

- Camerabeelden worden uitsluitend gebruikt ten behoeve van de doelstelling zoals genoemd in lid 2.

Artikel 3 – Taken en verantwoordelijkheden

- Het cameratoezicht geschiedt onder verantwoordelijkheid van het College van Bestuur.
- Alvorens te besluiten tot het instellen of intensiveren van cameratoezicht, voert het College van Bestuur een privacy toets uit, waarbij de mate van inbreuk op de privacy van de leerlingen, medewerkers en bezoekers wordt afgewogen tegen het belang van de onderwijsinstelling om cameratoezicht te gebruiken. Hierbij wordt meegewogen of de doelstellingen als geformuleerd in artikel 2, op een andere wijze kunnen worden bereikt, met een minder ingrijpend middel dan cameratoezicht.
- Het College van Bestuur wijst een beheerder aan die verantwoordelijk is voor de inrichting, het beheer en toezicht op het cameratoezicht binnen de onderwijsinstelling, alsmede een technisch beheerder die, onder verantwoordelijkheid van de beheerder, belast is met het technisch beheer van het camerasysteem. (Privacy officer Stichting VCO, Serve It bv)
- De beheerder wijst bevoegde medewerkers aan, en zo nodig een of meer locatiebeheerder(s).
- De beheerder wijst voor zichzelf en voor de locatiebeheerder een plaatsvervanger aan, die in geval van afwezigheid van de beheerder respectievelijk locatiebeheerder in diens taken en verantwoordelijkheden treedt.
- De beheerder, locatiebeheerder(s) en bevoegde medewerkers zijn bevoegd tot het live uitkijken van camerabeelden.
- De beheerder en locatiebeheerder zijn bevoegd tot het terugkijken en uitgeven van opgenomen camera- beelden.
- De beheerder en locatiebeheerder kunnen een bevoegde medewerker autoriseren (autorisatie loopt via technisch beheerder) om – onder verantwoordelijkheid van de beheerder of locatiebeheerder - onder nader te stellen voorwaarden en voor een vooraf bepaald doel c.q. een vooraf bepaalde periode camerabeelden terug te kijken.

Artikel 4 – Inrichten camerasysteem en beveiliging

- De beheerder en technisch beheerder zijn verantwoordelijk voor de inrichting van het camerasysteem en de plaatsing van de camera's, binnen de kaders van de door het College van Bestuur uitgevoerde privacy toets als bedoeld in artikel 3 lid 2.
- De technische beheerder zorgt voor passende technische en organisatorische maatregelen om de camerabeelden te beveiligen tegen verlies of tegen enige vorm van onrechtmatig gebruik.
- Het terugkijken van opgenomen camerabeelden geschiedt slechts in aanwezigheid van twee daartoe bevoegd verklaarde personen. De technisch beheer is niet bevoegd.
- De met cameratoezicht belaste medewerkers gaan vertrouwelijk en integer om met de kennis die zij tot zich krijgen vanwege het cameratoezicht, in het bijzonder met betrekking tot de privacy van leerlingen, medewerkers en bezoekers. Voor zover daar arbeidsrechtelijk niet in is voorzien, sluit de beheerder daartoe een geheimhoudingsverklaring met de locatiebeheerder(s), technisch beheerder en/of bevoegde medewerker(s).
- De beheerder draagt er zorg voor dat het cameratoezicht kenbaar wordt gemaakt aan leerlingen en/of hun wettelijk vertegenwoordiger, medewerkers en bezoekers op zichtbare en herkenbare wijze, zoals maar niet beperkt tot borden en stickers bij de ingang van de gebouwen of terreinen van de onderwijsinstelling.
- Voor zover er in het camerasysteem camerabeelden worden opgeslagen, worden deze beelden na uiterlijk vier weken na de opname automatisch gewist, tenzij er een incident is geconstateerd op basis waarvan het noodzakelijk is de met het incident samenhangende camerabeelden te bewaren. Na afhandeling van het incident worden de betreffende camerabeelden (en eventueel gemaakte kopieën of afdrukken) gewist.
- Het camerasysteem is zodanig uitgerust dat het terugkijken van opgenomen camerabeelden of het uitgeven daarvan slechts mogelijk is in een veilige en vertrouwde ruimte.
- Technisch beheerder krijgt een melding, per e-mail, als een gebruiker een video download of verwijderd. De technisch beheerder houdt contact met de beheerder van het cameratoezichtsysteem.
- Het is in de audit logboeken in te zien of iemand de app gebruikt heeft om beelden te bekijken. Dit gaat echter wel op audit logfile per school en dient handmatig te gebeuren.
- Voor zover er camerabeelden worden uitgekeken in een andere ruimte dan in een veilige en vertrouwde ruimte, zijn er technische en organisatorische maatregelen genomen die het onbevoegd meekijken zoveel als redelijkerwijs mogelijk voorkomen.
- Voor zover er bij het inrichten van het camerasysteem voor gekozen wordt om de leerlingen, medewerkers en bezoekers via een monitor live terugkoppeling te geven van de camerabeelden, kunnen deze live camerabeelden alleen betrekking hebben op deze betreffende leerlingen, medewerkers en bezoekers.
- Bewerking van camerabeelden vindt slechts plaats in het kader van het verscherpen van deze camerabeelden.

Artikel 5 – Inzage en uitgifte opgenomen camerabeelden aan derden

- Op verzoek van politie, rechter-commissaris of (hulp)officier van justitie kan inzage worden gegeven in (opgenomen) camerabeelden in het kader van de uitoefening van diens publiekrechtelijke taak.
- Uitgifte van camerabeelden vindt slechts plaats op *vordering* van de politie, rechter-commissaris of (hulp)officier van justitie waarbij de vordering gebaseerd is op een wettelijke grondslag.
- Alvorens tot inzage of uitgifte over te gaan, legitimeert de betreffende functionaris zich vooraf ten overstaan van de beheerder of locatiebeheerder, en tekent voor ontvangst van de uitgegeven camerabeelden.
- De inzage en uitgifte wordt door de beheerder of locatiebeheerder geregistreerd.
- Aan andere derden wordt geen inzage in de camerabeelden gegeven, of camerabeelden uitgegeven, anders dan met de uitdrukkelijke toestemming van de betrokken leerling en/of hun wettelijk vertegenwoordiger, medewerker of bezoeker.

Artikel 6 – Rechten van betrokkenen

- Betrokken leerlingen en/of hun wettelijk vertegenwoordiger, medewerkers en bezoekers komen de rechten toe zoals bedoeld in de Algemene Verordening Gegevensbescherming (tot 25 mei 2018 de Wet bescherming persoonsgegevens). Hieronder vallen het recht op inzage, correctie en verwijdering van camerabeelden waarop zij zijn afgebeeld.
- Een verzoek tot inzage in camerabeelden geschiedt schriftelijk of per e-mail aan de beheerder, die binnen 10 werkdagen na ontvangst van het verzoek inhoudelijk zal reageren.
- Het verzoek tot inzage wordt afgewezen wanneer het verzoek tot inzage in camerabeelden ongespecificeerd is, of als met dit verzoek kennelijk misbruikt van recht wordt gemaakt.
- In geval van een incident, kan een inzageverzoek worden geweigerd als dat noodzakelijk is in het belang van de voorkoming, opsporing en vervolging van strafbare feiten.
- (*voor zover er nog niet is voorzien in een universele klachtenregeling binnen VCO):* Klachten over de toepassing van het camerasysteem, dit reglement en over het gedrag van de beheerder, locatiebeheerder of de bevoegde medewerkers, worden schriftelijk ingediend bij het College van Bestuur. Het College van Bestuur zal binnen 6 weken na datum ontvangst van de klacht reageren.

Artikel 7 – Verslaglegging en rapportage

- De technische beheerder rapporteert de beheerder jaarlijks de rapporten welke op zijn beurt weer worden aangeboden aan het College van Bestuur over het toegepaste cameratoezicht, waaronder begrepen is een verslag over de verstrekkingen van camerabeelden zoals bedoeld in artikel 5.
- Jaarlijks wordt door het College van Bestuur gerapporteerd aan de (G)MR over het cameratoezicht betreffende het voorafgaande jaar (over aard, frequentie en lengte van het toezicht). Daarbij wordt specifiek gemeld indien (heimelijk) cameratoezicht is toegepast.

- Ieder jaar (schoolseizoen) wordt er in de maanden december en juni rapportage verstrekt door de technisch beheerder aan de beheerder van VCO. Gebaseerd op een geautomatiseerd ticketsysteem welke door Serve IT is aangemaakt.
- Elke locatie heeft zijn eigen inlograpportage. De inloggegevens worden onder geen enkele omstandigheid gedeeld met derden.
- Elk kwartaal wordt er door hoofd bedrijfsvoering in samenwerking met Serve IT een controle uitgevoerd. Hierbij wordt gecontroleerd wat de ingelogde personen bekeken hebben. Bij gebeurtenissen die niet regulier zijn, wordt de betreffende persoon bevraagd. Hier wordt een verslag van gemaakt welk toegevoegd wordt aan het logboek.

Artikel 8 – Slotbepaling

- Het College van Bestuur stelt dit reglement vast. Voorafgaand aan het vaststellen, wijzigen of intrekken van dit reglement cameratoezicht, vraagt het College van Bestuur de (G)MR om instemming.
- Het College van Bestuur informeert, indien aanwezig, de leerlingenraad over het vaststellen, wijzigen of intrekken van dit reglement.
- Het reglement treedt onmiddellijk in werking. Een wijziging in dit reglement treedt in werking binnen 30 dagen na bekendmaking van de wijziging.

School	Adres	Postcode & Plaats	Telefoonnr.
Leonardo,	Vliepad 5,	3844 EL Harderwijk	0341416645
CBS De Brug,	Piet Heinlaan 22,	3843 EZ Harderwijk	0341416576
CBS DOK 19,	Flevoweg 73,	3841 KK Harderwijk	0341416622
CBS De Rank,	Bongerdsteeg 3,	3841 CV Harderwijk	0341416748
CBS De Schakel 1,	Vondellaan 26,	3842 EH Harderwijk	0341416557
CBS De Schakel 2,	Busken Huetlaan 4,	3842 CS Harderwijk	0341416722
CBS De Triangel,	Tonselsedreef 60,	3845 CT Harderwijk	0341433965
CBS De Wegwijzer,	Kennedylaan 1,	3844 BA Harderwijk	0341416780
CBS Willem Alexander,	Veldkamp 33,	3843 BG Harderwijk	0341416770
CBS Het Startblok,	Beizenplein 2,	3845 KA Harderwijk	0341430921
CBS De Bron,	Frankenskamp 4,	3848 DE Harderwijk	0341426704
CBS De Parel,	Zuiderzeestraatweg 145,	3849 AD Hierden	0341451295
CBS Het Baken,	Vollenhovemeen 29,	3844 NC Harderwijk	0341422184

Facilitaircentrum	Adres	Postcode & Plaats	Telefoonnr.
't Schippertje	Kennedylaan 3,	3843 BG Harderwijk	0627013458

ECK-id

Aanmeldingsformulier

Bij de aanmelding van uw kind op onze school hebben wij een aantal gegevens nodig. Deze verkrijgen wij o.a. door het aanmeldformulier. De meeste vragen op dit aanmeldformulier spreken voor zich. Een aantal vragen zijn wij wettelijk verplicht aan u te stellen. De gegevens die u heeft ingevuld op het aanmeldformulier worden opgeslagen in de leerlingenadministratie van onze school. Uiteraard worden deze gegevens vertrouwelijk behandeld.
Op onze administratie is de AVG van toepassing. Dit betekent onder andere dat de gegevens door ons worden beveiligd en dat de toegang tot de administratie is beperkt tot alleen die medewerkers die de gegevens nodig hebben. U heeft als ouder het recht om de door ons geregistreerde gegevens in te zien (voor zover die informatie betrekking heeft op uw kind). Als de gegevens niet juist zijn, dan mag u van ons verwachten dat wij -op uw verzoek - de informatie verbeteren of aanvullen.

Basispoort

Om leerlingen eenvoudig toegang te geven tot het digitaal leermateriaal van zijn of haar school, maken al onze VCO-scholen gebruik van Basispoort. Dit maakt het geven van onderwijs op maat via gedigitaliseerde leermiddelen mogelijk. Hiervoor zijn echter leerlinggegevens nodig. VCO heeft met Basispoort een verwerkersovereenkomst afgesloten waarin afspraken zijn gemaakt over het gebruik van de leerlinggegevens.

ECK

Alle leerlingen van VCO hebben een unieke iD-code voor veilig inloggen en dagelijks gebruik van digitaal leermateriaal, het zogenoemde ECK iD. ECK staat voor Educatieve ContentKeten. Basispoort en alle ketenpartners die zijn aangesloten op de toegangsdiensten van Basispoort, gebruiken het ECK iD voor identificatie.
Het ECK iD is een versleuteld pseudoniem van het persoonsgebonden nummer met een eigen wettelijke basis.
Het ECK iD verbindt gebruikers en licenties van digitaal leermateriaal betrouwbaar en bestendig met elkaar. Hierdoor hoeven er geen herleidbare persoonsgegevens te worden gedeeld. ECK iD's worden aangemaakt door de Nummervoorziening. Dit is een publieke voorziening in beheer bij Kennisnet.

Telefoonlijst

In het kader van de wet op de privacy mogen wij als school geen contactgegevens van ouders met andere ouders delen. Daarom wisselen wij geen klassenlijsten met adressen van leerlingen uit. Wij vragen u als ouders daarom zelf met elkaar deze gegevens uit te wisselen mocht u daar behoefte aan hebben.

Functionaris gegevensbescherming

Wie

De Functionaris Gegevensbescherming (FG) is een onafhankelijk en deskundig persoon. De FG heeft als taak het toezicht houden op de toepassing en naleving van privacywetgeving. VCO heeft Privacy op School aangesteld als FG-functionaris.

Privacy op School
Stationsweg 1
3445 AA Woerden

Functionaris gegevensbescherming: Raoul Persoon

Verantwoordelijkheid FG-functionaris

De AVG stelt een aantal eisen aan de positie, taken en verantwoordelijkheden van de FG. De FG is in ieder geval verantwoordelijk voor het houden van onafhankelijk toezicht op, en adviseren van de VCO met betrekking tot de juiste en zorgvuldige omgang met persoonsgegevens. Dit betekent dat de FG bij alle mogelijke processen waar persoonsgegevens worden gebruikt betrokken is. Daarnaast loopt de formele communicatielijn van de organisatie naar de Autoriteit Persoonsgegevens met betrekking tot vragen en klachten over de verwerking van persoonsgegevens via de FG. Dit is ook de escalatielijn voor de FG als deze een escalatie nodig acht.

Plaats in de organisatie

Privacy is een breed onderwerp, wat vraagt om zorgvuldige bestuurlijke afweging van diverse belangen en risico's. De FG is de formele toezichthouder samen met de Autoriteit Persoonsgegevens. De FG rapporteert en adviseert rechtstreeks aan de bestuurder. Binnen de stichting is een Privacy officer aangesteld, die intern aanspreekpunt en verantwoordelijke is voor het privacy beleid. Door de onafhankelijke FG en de interne privacy officer borgt VCO de zorgvuldige omgang met persoonsgegevens en privacy.

Inzet van de FG en tool

De aanstelling van de FG is afgestemd op de aard van onze stichting, de gegevensverwerkingen en de daarbij behorende risico's. VCO maakt gebruik van de registratietool van Kennisnet. Dit is verwerkingssoftware die wordt ingezet voor de AVG en beschrijft de processen waarbij persoonsgegevens worden gebruikt.

Proces

Om de expertise van de FG optimaal te benutten, zijn er regelmatig contacten met de VCO. Bij het ontwikkelen van beleid, de aanschaf van andere software of aanpassingen in processen waarin persoonsgegevens worden verwerkt vervult de FG een adviserende rol.
Dit betekent niet dat de FG ook daadwerkelijk van al deze facetten zelf de expertise hoeft te hebben. Deze kennis kan ook elders in de VCO zijn belegd. VCO moet voldoende checks inbouwen in de processen om er zeker van te zijn dat de FG ook echt goed als adviseur en toezichthouder

betrokken kan zijn. Besluiten zonder een advies van de FG zijn dan ook niet mogelijk. Er moet steeds opnieuw worden gekeken naar de processen rond (het ontwerpen en uitvoeren van) gegevensverwerking en de rol van de FG.

Profiel

De Functionaris Gegevensbescherming beschikt over kennis en kunde om deze rol goed te kunnen vervullen. Een aantal belangrijke kwaliteiten zijn bijvoorbeeld:

- Bestuurlijk sensitief:
  Omdat de FG een adviesrol heeft en 'hoog' in de organisatie staat is het een belangrijke opgave om alle stakeholders te betrekken, te begrijpen wat bestuurlijke belangen zijn en hier op een zelfstandige wijze mee om te gaan.

- Communicatief sterk en diplomatiek:
  De regelgeving met betrekking tot persoonsgegevens vraagt een andere omgang hiermee. Het vraagt bewustwording en ander gedrag van ons. Dit zal mogelijk weerstand oproepen. De FG heeft daarom overtuigingskracht nodig, moet kunnen netwerken, draagvlak kunnen creëren en het belang van gegevensbescherming kunnen overbrengen.

- Inhoudelijk expert:
  De FG heeft kennis op het gebied van de AVG en andere wetgeving over gebruik van informatie en data door de overheid, maar ook als het gaat om bijvoorbeeld informatietechnologie. Bovendien is onze FG goed op de hoogte van de processen binnen de VCO en van de gegevensverwerking

Gedragscode AVG voor leerlingen

Gedragscode voor het omgaan met persoonsgegevens voor leerlingen

1. Wij mogen je gegevens alleen gebruiken als het mag Wij mogen jouw gegevens alleen bewaren en gebruiken als dit volgens de wet mag. Meestal vragen we eerst toestemming van jou of van je ouders.
2. Wij houden bij wat we met je gegevens doen We houden alles bij; van welke gegevens we van jou hebben en waarom we ze nodig hebben. Dit is zodat we kunnen laten zien dat we je gegevens op een goede manier gebruiken.
3. We vragen om toestemming Wij vragen altijd om jouw toestemming (of die van je ouders) voordat we jouw gegevens bewaren. We zorgen ervoor dat het duidelijk is dat jij het ermee eens bent.
4. Jij hebt het recht om je gegevens te bekijken en te veranderen Jij (of je ouders) mag kijken welke gegevens we van jou hebben. Als iets niet klopt, mag je ons vragen het te veranderen of weg te halen.
5. Je kunt je gegevens makkelijk meenemen Als je naar een andere school gaat, zorgen we ervoor dat je de gegevens die we van jou hebben makkelijk mee kunt nemen.
6. We zorgen voor privacy We kijken altijd goed of de manier waarop we je gegevens gebruiken veilig is. Als we denken dat er risico's zijn, nemen we maatregelen om het veiliger te maken.
7. Er is iemand die toeziet op je gegevens We hebben iemand die zorgt dat we jouw gegevens veilig bewaren en gebruiken. Wij zorgen ervoor dat alles goed wordt gecontroleerd.
8. Als er een probleem is met je gegevens, melden we het Als er iets misgaat met je gegevens, zoals als iemand er toegang toe krijgt die dat niet mag, dan melden we dat meteen en zorgen we ervoor dat het opgelost wordt.
9. We werken goed samen met anderen die jouw gegevens verwerken Als we met anderen samenwerken die jouw gegevens verwerken (bijvoorbeeld een andere school of organisatie), maken we duidelijke afspraken om jouw gegevens goed te beschermen.

Wat vragen wij van jou als leerling (en van ouders)?

1. Maak geen foto's of video's zonder toestemming Maak geen foto’s of video's van andere leerlingen, leraren of medewerkers zonder eerst toestemming te vragen. Dit geldt ook voor foto's die je op social media deelt.
2. Gebruik geen gegevens van anderen zonder toestemming Je mag de persoonlijke gegevens van andere leerlingen of medewerkers niet gebruiken zonder hun toestemming. Dit betekent bijvoorbeeld niet zomaar hun naam, adres of andere persoonlijke informatie delen.
3. Wees voorzichtig met het delen van gegevens online Deel geen persoonlijke gegevens zoals je adres, telefoonnummer of wachtwoorden op internet, tenzij je zeker weet dat het veilig is en je toestemming hebt van je ouders of de school.
4. Respecteer de privacy van anderen Iedereen heeft recht op privacy. Respecteer dus de persoonlijke ruimte en gegevens van anderen. Stel niet ongevraagd vragen over persoonlijke zaken.

5. Meld problemen of ongewenst gedrag Als je merkt dat iemand anders zich niet aan de privacyregels houdt, of als er iets misgaat met jouw gegevens, laat het dan weten aan een leraar of andere volwassene op school.
6. Gebruik je schoolaccounts op een verantwoorde manier Als je inlogt op computers of online platforms die de school gebruikt, doe dit dan op een veilige manier. Deel je wachtwoorden nooit met anderen en zorg ervoor dat je altijd netjes omgaat met de informatie die je online vindt.
7. Denk na over wat je deelt in digitale gesprekken Als je online met andere leerlingen praat, wees dan voorzichtig met het delen van persoonlijke informatie. Denk er altijd aan dat je niet weet wie het gesprek kan meelezen.

Grondslagen VCO

Algemene informatie grondslagen

VCO heeft goede reden om persoonsgegevens te verwerken. In de privacywet, de Algemene verordening gegevensbescherming (AVG), staan 6 redenen genoemd. De juridische naam voor die redenen is grondslagen. VCO heeft dus een grondslag nodig om persoonsgegevens te mogen verwerken.

VCO bepaalt steeds welke grondslag van toepassing is. VCO bepaalt de grondslag voordat wordt begonnen met gegevens verwerken.

De 6 grondslagen

In de AVG staan de volgende 6 grondslagen voor het verwerken van persoonsgegevens:

- U heeft toestemming van de persoon om wie het gaat.
- Het is noodzakelijk om gegevens te verwerken om een overeenkomst uit te voeren.
- Het is noodzakelijk om gegevens te verwerken omdat u dit wettelijk verplicht bent.
- Het is noodzakelijk om gegevens te verwerken om vitale belangen te beschermen.
- Het is noodzakelijk om gegevens te verwerken om een taak van algemeen belang of openbaar gezag uit te oefenen.
- Het is noodzakelijk om gegevens te verwerken om uw gerechtvaardigde belang te behartigen.

VCO heeft dus een grondslag nodig voor verwerking van persoonsgegevens. VCO moet kunnen onderbouwen waarom voor deze grondslag is gekozen.
Let op: deze regels gelden alleen voor gewone persoonsgegevens. Wilt u bijzondere persoonsgegevens verwerken? Zoals gegevens over iemands gezondheid? Of strafrechtelijke gegevens? Dat is verboden. Tenzij u voldoet aan een aantal strenge eisen. Een grondslag hebben is dan dus niet genoeg.

Persoonlijk gebruik

Verwerking van persoonsgegevens die verkregen zijn via VCO mogen niet persoonlijk gebruikt worden. Je mag bijvoorbeeld geen adressen van leerlingen of medewerkers uit het systeem halen om deze privé te gebruiken.

Grondslag toestemming

Een van de grondslagen in de AVG is dat mensen toestemming hebben gegeven om hun persoonsgegevens te verwerken.
In de AVG staat een aantal eisen waaraan toestemming moet voldoen. Voldoet de toestemming niet aan deze eisen? Dan is de toestemming niet geldig. De persoonsgegevens mogen dan niet verwerkt worden.

Toestemming moet voldoen aan de volgende eisen:

- Vrijelijk gegeven

- Ondubbelzinnig
- Geïnformeerd
- Specifiek
- Iemand mag niet onder druk worden gezet om toestemming te geven. Bijvoorbeeld door iemand te benadelen als diegene geen toestemming geeft. Let daarbij op machtsverhoudingen. Werknemers kunnen een vraag van hun werkgever bijvoorbeeld moeilijk weigeren.

Ondubbelzinnig

Er moet sprake zijn van een duidelijke actieve handeling om toestemming te geven. Bijvoorbeeld een (digitale) schriftelijke of een mondelinge verklaring. Het moet in elk geval heel helder zijn dat er toestemming is gegeven.
Er mag niet van worden uitgegaan dat iemand impliciet toestemming geeft. Het gebruik van vooraf aangevinkte vakjes is dus niet toegestaan.

Geïnformeerd

Mensen moeten worden geinformeerd over:

- de identiteit van de organisatie;
- het doel van elke verwerking waarvoor toestemming wordt gevraagd;
- welke persoonsgegevens worden verzameld en gebruikt;
- het recht dat mensen hebben om de toestemming weer in te trekken.
- de informatie voor het vragen van toestemming moet in een toegankelijke vorm aangeboden worden. Ook moet deze begrijpelijk zijn, zodat iemand een weloverwogen keuze kan maken. Dat betekent dat er duidelijke en eenvoudige taal moet worden gebruikt.

Specifiek

Toestemming moet steeds gelden voor een specifieke verwerking en een specifiek doel. Zijn er meerdere doeleinden om gegevens te verwerken? Dan moet de betrokkene hierover geinformeerd worden en voor elk doel afzonderlijk toestemming geven. Het doel mag niet gaandeweg veranderen.

Toestemming vragen

De AVG schrijft niet precies voor in welke vorm toestemming moet worden gevraagd. Hier is een vrije keuze in. Een van de manieren om toestemming te vragen is de betrokkene een schriftelijke verklaring laten invullen en ondertekenen.
In een online omgeving kunnen mensen worden gevraagd om toestemming door bijvoorbeeld:

- actief een vakje aan te vinken;
- op een knop of een link te klikken;
- een elektronisch formulier in te vullen;
- een e-mail aan u te sturen;
- een elektronische handtekening te zetten;
- een gescand document met handtekening te uploaden.
- Een mondelinge verklaring kan ook voldoende zijn om geldige toestemming te krijgen. Maar hierbij kan het moeilijk te bewijzen zijn dat er daadwerkelijk toestemming is gegeven.

- Er kan toestemming worden gekregen met een opgenomen telefoongesprek. Er moet daarbij dan wel duidelijke informatie gegeven worden en om een specifieke bevestiging vragen van de persoon. Bijvoorbeeld dat iemand een knop indrukt of duidelijk 'ja' of 'nee' zegt.

Aantonen toestemming gegeven is

Volgens de AVG heeft de VCO een verantwoordingsplicht. Om geldige toestemming aan te tonen, moet VCO niet alleen de toestemming zelf vastleggen. Zij moet ook kunnen laten zien op basis van welke informatie iemand de toestemming heeft gegeven.

Vraagt VCO online toestemming aan mensen voor het verwerken van hun persoonsgegevens? Dan kan VCO de informatie vastleggen over het websitebezoek waarin zij de toestemming hebben gegeven. Deze informatie kan gecombineerd worden met:

- documentatie over de manier waarop VCO toestemming ontvangt en vastlegt;
- een kopie van de informatie die de betrokkenen hebben ontvangen voordat zij toestemming gaven.

Tot slot moet VCO ervoor zorgen dat u voldoende data heeft waarmee u een link tussen de verwerking en de toestemming van een betrokkene kunt aantonen. Let wel op dat u hierbij niet meer data mag verzamelen dan daarvoor noodzakelijk is.

Toestemming ingetrokken

Mensen hebben het recht om hun toestemming in te trekken. Dat moet even makkelijk gaan als toestemming geven. Wij zorgen er dus voor dat mensen hun toestemming eenvoudig kunnen intrekken.

Toestemming bij kinderen

VCO verwerkt persoonsgegevens van kinderen. Wij letten extra op onderstaande punten:

- **Bied extra bescherming >** De AVG geeft kinderen jonger dan 16 jaar extra bescherming. Want kinderen kunnen de risico's van een gegevensverwerking niet of minder goed inschatten.
- **Zorg voor geldige toestemming >** Kinderen jonger dan 16 jaar kunnen zelf geen geldige toestemming geven voor het verwerken van hun gegevens. Ouders en/of verzorgers geven deze toestemming voor online en offline verwerking van persoonsgegevens. Toestemming is alleen geldig als een van de ouders of verzorgers van een kind deze geeft.

Controleer wie toestemming heeft gegeven

VCO is verplicht om te controleren of de toestemming is gegeven door één van de ouders of verzorgers van het kind. Dit moet aangetoond kunnen worden wanneer de Autoriteit Persoonsgegevens ernaar vraagt.

Uitdrukkelijke toestemming

Wanneer bijzondere persoonsgegevens verwerkt worden, is de uitdrukkelijke toestemming van die persoon nodig.
Let op: Bepaalt de wet al dat u bijzondere persoonsgegevens mag verwerken? Dan heeft u niet ook nog eens uitdrukkelijke toestemming nodig.

Uitdrukkelijke toestemming is een verzwaarde vorm van toestemming. Daarmee is uitdrukkelijke toestemming (art. 9 AVG) iets anders dan de 'normale', ondubbelzinnige toestemming die een van de 6 grondslagen is om gegevens te mogen verwerken (art. 6 AVG).

Voor uitdrukkelijke toestemming is meer vereist dan voor ondubbelzinnige toestemming. De term 'uitdrukkelijk' verwijst naar de manier waarop betrokkenen hun toestemming tot uitdrukking brengen.
Het betekent dat de betrokkene een uitdrukkelijke verklaring van toestemming moet geven. Bijvoorbeeld door een geschreven verklaring te ondertekenen.

Grondslag overeenkomst

Eén van die grondslagen in de AVG is dat het noodzakelijk is om persoonsgegevens te verwerken om een overeenkomst uit te voeren. Dit houdt het volgende in:

VCO mag zich op deze grondslag baseren als zij een overeenkomst heeft met iemand en hiervoor het verwerken van persoonsgegevens noodzakelijk is.
De overeenkomst zelf mag niet gericht zijn op het verwerken van persoonsgegevens, maar moet een ander doel hebben. Deze grondslag geldt ook voor een fase voordat er een overeenkomst afgesloten wordt. Bijvoorbeeld bij het op verzoek een offerte opstellen.
Let op dat er geen persoonsgegevens verwerkt worden die niet noodzakelijk zijn om de overeenkomst uit te voeren.

Grondslag wettelijke verplichting

Is de verwerking van de persoonsgegevens noodzakelijk om aan een wettelijke verplichting te voldoen? Dan kan VCO zich op deze grondslag baseren.

Bijvoorbeeld: VCO heeft een bevel van de politie om bepaalde persoonsgegevens aan de politie te verstrekken.

Het hoeft niet expliciet in de wet te staan dat VCO persoonsgegevens moet verwerken om een specifieke taak uit te voeren. Soms is de verplichting in de wet namelijk ruimer geformuleerd. Het is dan aan VCO om te bepalen of het verwerken van persoonsgegevens noodzakelijk is om aan de verplichting te voldoen.

VCO kan zich niet op deze grondslag baseren als het gaat om een zeer algemene taak. Zoals het handhaven van de openbare orde. Daarvoor geldt een andere grondslag, namelijk de grondslag van algemeen belang of openbaar gezag.

Grondslag vitaal belang

VCO kan zich maar in enkele gevallen op deze grondslag baseren.
Een vitaal belang is aan de orde als het over een belang gaat dat essentieel is voor iemands leven of gezondheid. En die persoon niet om toestemming gevraagd kan worden om gegevens te verwerken. Bijvoorbeeld wanneer er acuut gevaar dreigt, maar iemand bewusteloos is of mentaal niet in staat om toestemming te geven.
Een voorbeeld: bij een incident op school moet de hulpverlening onmiddellijk op gang komen. In die situatie is het onmogelijk om eerst alle betrokken personen te informeren en om toestemming te vragen om hun medische gegevens te verwerken.

Grondslag algemeen belang of openbaar gezag

Is de verwerking noodzakelijk om een publieke taak uit te oefenen voor het algemeen belang of openbaar gezag? Dan kan VCO zich op deze grondslag baseren. Het gaat daarbij om taken die in de wet zijn vastgelegd en die relevant zijn voor de organisatie.
Het moet voor mensen ook duidelijk zijn dat VCO hun persoonsgegevens verwerkt om die specifieke wettelijke taak uit te oefenen. Daarnaast moet de verwerking van de persoonsgegevens noodzakelijk zijn om de publieke taak goed te kunnen vervullen.

Grondslag gerechtvaardigd belang

Om de verwerking te mogen baseren op de grondslag 'noodzakelijk voor de behartiging van een gerechtvaardigd belang', moet aan 3 voorwaarden voldaan worden. Hiermee toetst VCO of het recht om persoonsgegevens te verwerken – omdat er een gerechtvaardigd belang is om dit te doen – zwaarder weegt dan iemands recht op privacy.

De 3 voorwaarden zijn:

- VCO heeft daadwerkelijk een gerechtvaardigd belang. Niet elk belang kwalificeert als een gerechtvaardigd belang.
- De verwerking is noodzakelijk om dit belang te behartigen.
- VCO heeft een afweging gemaakt tussen uw belangen en die van de betrokkenen.

Voorwaarde 1: gerechtvaardigd belang

Het belang is echt een gerechtvaardigd belang als het ergens in het recht is opgenomen. En wordt erkend en beschermd. Dat mag ook in een ongeschreven rechtsregel of rechtsbeginsel zijn. Als het maar gaat om een belang waarvan we in de maatschappij vinden dat het door het recht beschermd moet worden.
Dit kwalificeert bijvoorbeeld niet als gerechtvaardigd belang:

- een puur commercieel belang;
- winstmaximalisatie;
- het gedrag van werknemers volgen zonder legitieme reden;
- het (koop)gedrag van (potentiële) klanten volgen zonder legitieme reden.

Is er geen gerechtvaardigd belang? Dan kan de verwerking niet gebaseerd worden op deze grondslag.

Voorwaarde 2: noodzakelijkheid

Is er daadwerkelijk een gerechtvaardigd belang? Dan moet er vervolgens gekeken worden of de verwerking van persoonsgegevens noodzakelijk is om dit belang te behartigen. Ga hiervoor het volgende na:

Staat het doel van de verwerking in verhouding tot de inbreuk op de privacy van de betrokkenen. In de AVG heet dit 'proportionaliteit'. Kan het doel niet worden bereikt op een manier die minder ingrijpend is voor de betrokkenen. In de AVG heet dit 'subsidiariteit'. Wanneer aan beide eisen wordt voldaan is de verwerking noodzakelijk.

Voorwaarde 3: afweging belangen

Is er een gerechtvaardigd belang en is de gegevensverwerking noodzakelijk om dit belang te behartigen? Dan moet VCO tot slot een afweging maken tussen haar belangen en de belangen van de betrokkenen.

Bij deze afweging wordt gekeken naar:

- de gevolgen voor de betrokkenen;
- hoe ernstig de inbreuk is op de privacy van de betrokkenen;
- welke (aanvullende) maatregelen zijn genomen om ongewenste gevolgen voor de betrokkenen te voorkomen of beperken;
- of de betrokkenen de verwerking min of meer kunnen verwachten. Bijvoorbeeld als vervolg op een eerdere verwerking waarvoor zij toestemming hebben gegeven of als vervolg op verwerkingen die noodzakelijk zijn om een contract uit te voeren.

Let op: Wilt u persoonsgegevens verwerken van kinderen (jonger dan 16 jaar)? Dan weegt het gerechtvaardigd belang van de organisatie minder snel op tegen hun rechten en vrijheden.

De afweging kan tot 2 conclusies leiden:

1. De belangen van de betrokkene blijken zwaarder te wegen. VCO kan de verwerking hierdoor niet baseren op de grondslag gerechtvaardigd belang. De gegevens mogen dus niet verwerkt worden.
2. De belangen van VCO wegen zwaarder. Er is hierdoor een grondslag om persoonsgegevens te verwerken. De gegevens mogen dus wel verwerkt worden.

Voorbeelden gerechtvaardigd belang

Een gerechtvaardigd belang kan bijvoorbeeld zijn:

- een veilig en gezond leven hebben of eigendommen beschermen in een dreigende situatie;
- de privésfeer beschermen;
- procederen en/of een rechtsvordering instellen, uitoefenen of onderbouwen;
- grensoverschrijdend gedrag in werkrelaties onderzoeken en beëindigen;
- fraude, oplichting of ander onrechtmatig gedrag tegengaan;
- iemand aansprakelijk stellen voor schade;
- computersystemen goed beveiligen en beschermen;
- zorgplichten nakomen voor werknemers en/of klanten;

- aan alle (zorg)verplichtingen voldoen die u heeft op basis van bijvoorbeeld het Burgerlijk Wetboek.

Het belang moet hierbij wel:

- echt zijn > dit houdt in dat het niet mag gaan om een mogelijk belang in de toekomst, wat niet zeker is
- concreet zijn > dit houdt in dat het belang duidelijk kunt verwoord kan worden
- rechtstreeks zijn > dit houdt in dat het gaat om een belang van VCO, dus niet een algemeen belang van 'de samenleving' of iets dergelijks.

Speciale regels voor bijzondere persoonsgegevens

De verwerking van bijzondere persoonsgegevens is meestal verboden. In de AVG staan 10 uitzonderingen. Dat betekent dat het verbod niet voor geldt wanneer VCO zich kan baseren op een uitzondering én op een van de grondslagen voor het verwerken van 'gewone' persoonsgegevens. In de praktijk vallen sommige van die uitzonderingen en grondslagen samen.

Van de 10 uitzonderingen uit de AVG zijn er 5 die alleen van toepassing zijn als hiervoor in de nationale wet een rechtsbasis is gecreëerd. Dat betekent dat VCO zich alleen op zo'n uitzondering kan beroepen als er in een Nederlandse wet staat dat dit mag.

De 10 uitzonderingen zijn:

1. Iemand heeft uitdrukkelijk toestemming gegeven voor de verwerking van de eigen persoonsgegevens.
2. Alleen als het in een wet staat: De verwerking is noodzakelijk om verplichtingen uit te voeren of specifieke rechten uit te oefenen van VCO of de betrokken persoon. Dit op het gebied van het arbeidsrecht, het socialezekerheidsrecht en het sociale beschermingsrecht.
3. De verwerking is noodzakelijk om de vitale belangen van de betrokken persoon of van een andere natuurlijke persoon te beschermen. Dit geldt alleen wanneer diegene fysiek of juridisch niet in staat is om toestemming te geven.
4. De gegevens worden verwerkt als stichting, vereniging of andere instantie zonder winstoogmerk die op politiek, levensbeschouwelijk, godsdienstig of vakbondsgebied werkzaam is. Het gaat om gegevens van (oud)leden of personen met wie regelmatig contact is, gerelateerd aan de doelstelling.
5. De verwerking van persoonsgegevens die de betrokkene zelf doelbewust openbaar heeft gemaakt.
6. De verwerking is noodzakelijk om een rechtsvordering in te stellen, uit te oefenen of te onderbouwen.
7. Alleen als het in een wet staat: De verwerking is noodzakelijk voor een zwaarwegend algemeen belang.
8. Alleen als het in een wet staat: De verwerking is noodzakelijk voor doeleinden van preventieve of (arbeids)geneeskundige aard. Zoals het beoordelen van arbeidsgeschiktheid en/of het verstrekken van gezondheidszorg.
9. Alleen als het in een wet staat: De verwerking is noodzakelijk voor de volksgezondheid.

10. Alleen als het in een wet staat: De verwerking is noodzakelijk voor archivering in het algemeen belang, wetenschappelijk/historisch onderzoek of statistische doeleinden.

Speciale regels voor strafrechtelijke gegevens

De verwerking van strafrechtelijke gegevens (AVG: persoonsgegevens van strafrechtelijke aard) is verboden. Tenzij er een beroep kan worden gedaan op een specifieke wettelijke uitzondering én op een van de grondslagen voor het verwerken van 'gewone' persoonsgegevens.

Dit zijn de 2 belangrijkste wettelijke uitzonderingen voor het verwerken van strafrechtelijke persoonsgegevens:

1. De verwerking staat onder toezicht van de overheid.
2. De verwerking is toegestaan bij nationaal recht. Het gaat dan om Unierechtelijke of lidstaatrechtelijke bepalingen, die passende waarborgen bieden voor de rechten en vrijheden van de betrokken personen.

Informatiebeveiliging en privacy (IBP)

Onze school zit in het tijdperk van digitale vooruitgang en toenemende afhankelijkheid van technologie. Wij erkennen de cruciale rol die informatiebeveiliging en privacy spelen in het handhaven van de integriteit van het onderwijsproces. Om te voldoen aan de Algemene Verordening Gegevensbescherming (AVG) hebben wij beleid op gebied van informatiebeveiliging en privacy (IBP). Het IBP beleid is erop gericht om de kwaliteit van de verwerking van informatie en de beveiliging van persoonsgegevens te optimaliseren. Hierbij moet er een juiste balans zijn tussen privacy, functionaliteit en veiligheid.

Doelstellingen van Informatiebeveiliging en Privacy op school

a) Bescherming van Persoonsgegevens: Wij verbinden ons ertoe de persoonlijke gegevens van onze leerlingen, ouders en medewerkers te beschermen tegen ongeoorloofde toegang, gebruik of openbaarmaking.
b) Veilige technologische Infrastructuur: We investeren in geavanceerde technologieën, handhaven en gebruiken up-to-date beveiligingsprotocollen om ervoor te zorgen dat onze digitale infrastructuur robuust en veilig is.
c) Bewustmaking en educatie: We streven naar het bevorderen van bewustzijn en educatie met betrekking tot informatiebeveiliging en privacy binnen onze school, zodat alle betrokkenen op de hoogte zijn van de risico's en beste praktijken.

Maatregelen voor Informatiebeveiliging binnen onze school

a) Toegangsbeheer: Wij implementeren strikte toegangscontroles om ervoor te zorgen dat alleen geautoriseerde personen toegang hebben tot persoonlijke informatie.
b) Versleuteling: Gevoelige gegevens worden versleuteld om ervoor te zorgen dat zelfs in geval van ongeoorloofde toegang, de informatie onleesbaar blijft.
c) Regelmatige Audits: Periodieke beveiligingsaudits worden uitgevoerd om de effectiviteit van onze beveiligingsmaatregelen te beoordelen en eventuele zwakke punten aan te pakken.

Privacybeleid binnen onze school

a) Transparantie: Wij informeren onze leerlingen, ouders, medewerkers en relaties duidelijk over welke gegevens worden verzameld, met welk doel en hoe deze worden verwerkt.
b) Voor elke vorm van gegevensverwerking verkrijgen we de benodigde toestemming van betrokkenen, en we respecteren het recht op intrekking van toestemming.
c) Gegevensminimalisatie: We beperken de verzameling van persoonsgegevens tot wat strikt noodzakelijk is voor het vervullen van het onderwijsproces op onze school.

Als school dragen wij de verantwoordelijkheid voor het handhaven van de hoogste normen op het gebied van informatiebeveiliging en privacy. U kunt het IBP beleid vinden op www.stichtingvco.nl/privacy/IBP

Privacy statement leerlingen

Inleiding

Alle twaalf basisscholen van de stichting voor christelijk onderwijs Harderwijk-Hierden (VCO) verwerken de persoonsgegevens van leerlingen en van ouders en/of verzorgers. Dit is bijvoorbeeld nodig om de leerlingen aan te melden en in te schrijven en om onderwijs te verzorgen. Voor zover de basisscholen zelfstandig voor eigen doeleinden persoonsgegevens verwerken, zijn wij hiervoor als VCO verwerkingsverantwoordelijke. Dit betekent dat we ons moeten houden aan de relevante verplichtingen uit de geldende privacywetgeving. Vanaf 25 mei 2018 is dit onder andere de Algemene Verordening Gegevensbescherming (AVG) en de Uitvoeringswet bij de AVG. Daarnaast gelden er specifieke verplichtingen ten aanzien van het verwerken van persoonsgegevens uit onder andere de Wet op het Primair Onderwijs.

Een van de verplichtingen uit de AVG is de informatieplicht. Als verwerkingsverantwoordelijke moeten we u informeren over de wijze waarop we persoonsgegevens verwerken. Door middel van dit Privacy-statement informeren wij u hierover.
In dit statement onderwijs hebben wij de meest voorkomende verwerkingen ten aanzien van het verzorgen van onderwijs beschreven in overeenstemming met de eisen die de AVG aan een Privacy-statement stelt.

VCO & Privacy statement

Zoals elke Stichting, vereniging en/of school in het Primair Onderwijs verwerkt VCO persoonsgegevens van onze leerlingen en hun ouder(s) of verzorger(s). Wij vinden het belangrijk u hierover duidelijkheid te geven. In dit Privacy-statement leggen wij uit hoe wij omgaan met persoonsgegevens van u en van uw kind(eren).
Onder VCO vallen de volgende scholen:

- CBS Het Baken
- CBS De Bron
- CBS De Brug
- DOK 19
- Leonardo Onderwijs
- CBS De Parel
- CBS De Rank
- CBS De Schakel
- CBS Het Startblok
- CBS De Triangel
- CBS De Wegwijzer
- CBS de Willem Alexanderschool

Contactgegevens

VCO, gevestigd aan de Veldkamp 33, 3843 BG te Harderwijk treedt op als bestuurder (met een RvT). VCO kan voor bepaalde gegevensverwerkingen ook als verwerkingsverantwoordelijke optreden. Dit lichten wij in dit Privacy-statement verder toe.

Op wie is dit Privacy Statement van toepassing?

Dit Privacy-statement is voor u van toepassing wanneer u uw kind aanmeldt bij de stichting/school en wanneer uw kind onderwijs volgt bij ons. Dit Privacy-statement geeft u als ouder of verzorger informatie over de verwerking van persoonsgegevens van uw kind en van uzelf.

Welke persoonsgegevens verwerken wij?

Wij maken onderscheid tussen verschillende gegevensverwerkingen die wij uitvoeren om onderwijs te kunnen aanbieden. Hieronder lichten wij toe welke (categorieën) van persoonsgegevens wij verwerken. *(Vanaf nu hebben wij het over één van onze scholen)*

Aanmelding bij ons op school.

Wij vragen u bij aanmelding (*let op, dit is nog geen definitieve inschrijving*) om verschillende persoonsgegevens in te vullen zoals aangegeven op het Aanmeldingsformulier Leerlingen. Wij vragen u in elk geval om de volgende persoonsgegevens:

A Persoonsgegevens van uw kind. Voor- en achternaam, geslacht, geboortedatum, geboorteplaats, adres en woonplaats, BSN (of tijdelijk onderwijsnummer), land van herkomst, datum in Nederland, culturele achtergrond, gegevens over voorschoolse educatie, school van herkomst, datum aanmelding (eventuele medicijnen en/of allergieën). U kunt hierbij ook aangeven of uw kind extra ondersteuning nodig heeft.
(*Er mag* ***GEEN*** *kopie gemaakt wordt van een paspoort of identiteitskaart. Alleen het BSN mag worden overgenomen)*

B Persoonsgegevens van u. Voor- en achternaam, geslacht, geboortedatum, geboorteplaats, land van herkomst, adres en woonplaats, waar u werkt, telefoonnummers, burgerlijke staat, e-mail adres, gegevens over de gezinssamenstelling, huisarts en verzekering.

Gegevens nodig voor het geven van onderwijs en begeleiding.

Om onderwijs te kunnen verzorgen registreren wij gegevens over de vorderingen van uw kind op school, zoals de jaargroep, cijfers en voortgangsrapporten. Ook houden wij een verzuimregistratie bij. Wij stellen bij het verlaten van de school een onderwijskundig rapport op over de schoolvorderingen en leermogelijkheden van uw kind. Hierin staan gegevens over resultaten, ontwikkelingen, gedrag en verzuim. Wij kunnen ook een schooladvies en score van landelijke toetsen (zoals Cito) vastleggen. Soms is het nodig om bijzondere persoonsgegevens te verwerken om uw kind beter te kunnen begeleiden, waaronder medische gegevens (zoals over dyslexie, ADHD of over een allergie).

Wij kunnen ook persoonsgegevens verwerken die noodzakelijk zijn om (digitale) leermiddelen aan te bieden. Het kan daarbij bijvoorbeeld gaan om een inlognaam en wachtwoord, een IP adres van de school, de groep waarin uw kind zit en het niveau dat uw kind heeft. Verder kunnen wij persoonsgegevens van u en uw kind verwerken die verband houden met uw contact met de school, bijvoorbeeld wanneer u vragen of klachten aan ons heeft gericht of ten aanzien van bepaalde taken die u voor de school uitvoert. Wanneer u betaling verricht aan de school, kunnen wij uw bankgegevens (IBAN) verwerken.

Waarvoor gebruiken wij persoonsgegevens?

Wij gebruiken de persoonsgegevens van u en uw kind voor verschillende doeleinden. Wij zetten ze voor u op een rij:

1. Om uw kind in te schrijven op onze school, ten behoeve van de toelating en plaatsing van uw kind op onze school. Voor het organiseren van onderwijs door ons en het geven van onderwijs en begeleiding aan uw kind, het geven van adviezen over onderwijs op basis van vorderingen van uw kind. Wij zijn in dit verband onder andere verplicht om bepaalde gegevens vast te leggen in een leerling volgsysteem.

   - Om u op de hoogte te houden over de voortgang van uw kind.
   - Om, al dan niet samen met VCO, (digitale) onderwijsmaterialen en leermiddelen aan te bieden.
   - Ten behoeve van de overgang van uw kind van onze school naar een andere onderwijsinstelling.
   - Voor het berekenen, vastleggen en innen van de vrijwillige ouderbijdrage.
   - Ten behoeve van interne en externe communicatie van en over de school, zoals de schoolgids of een nieuwsbrief.
   - Ten behoeve van buitenschoolse activiteiten zoals schoolreisjes.
   - Om ouders in de gelegenheid te stellen om contact met elkaar op te nemen.
   - Ten behoeve van de samenwerking van de scholen binnen VCO en de verplichtingen die daaruit voortvloeien.
   - Om uw vragen te kunnen beantwoorden en eventuele klachten af te handelen, en deze in voorkomend geval voor te leggen aan VCO.
   - Om samen met VCO leerlingen een passende en veilige leeromgeving te bieden, zowel fysiek als digitaal.
   - Om te voldoen aan de wettelijke verplichtingen die op ons en/of op VCO rusten, waaronder verplichtingen uit hoofde van de Wet op het Primair Onderwijs.

Wat is de grondslag voor de verwerking van de persoonsgegevens?

Wij verwerken alleen persoonsgegevens wanneer daarvoor een wettelijke grondslag aanwezig is.

- Toestemming.

Wij kunnen u in bepaalde gevallen vragen om toestemming te geven voorafgaand aan de gegevensverwerking. Zo zullen wij u vragen of wij uw contactgegevens kunnen opnemen in de klassenlijst en heeft u de mogelijkheid om aan te geven of uw adres en telefoonnummer geheim zijn. Ook vragen wij uw toestemming voor het gebruik van foto's van uw kind in de schoolgids, brochure of kalender, nieuwsbrief, op onze website of op onze sociale media accounts. U kunt uw toestemming te allen tijde intrekken door contact met ons op te nemen via de u bekende contactgegevens. Tenslotte vragen wij uw toestemming om de persoonsgegevens van uw kind door te geven aan de bibliotheek, wanneer u via ons van de diensten van de bibliotheek gebruik wil maken.

- Wettelijke verplichting.

Wij zijn in sommige gevallen verplicht om bepaalde persoonsgegevens van uw kind te verwerken. Deze verplichting kan ook meebrengen dat wij verplicht zijn bepaalde persoonsgegevens te delen met VCO voor verdere verwerking Zo zijn wij verplicht om een leerlingvolgsysteem te gebruiken om de vorderingen en resultaten bij te houden van onze leerlingen. Daarnaast zijn wij zoals iedere school verplicht om een onderwijskundig rapport op te stellen wanneer uw kind naar een andere school gaat. Tenslotte hebben wij bepaalde wettelijke verplichtingen ten aanzien van de kwaliteit van het onderwijs dat wij aanbieden. Ook hiervoor kan het noodzakelijk zijn om persoonsgegevens van u en uw kind te verwerken.

- Taak van algemeen belang.

Het kan noodzakelijk zijn om persoonsgegevens te verwerken over uw kind ten behoeve van de uitvoering van een taak van algemeen belang die op ons en/of VCO rust. Dergelijke taak bestaat hoofdzakelijk uit het organiseren van onderwijs en begeleiding. Het kan ook voorkomen dat wij persoonsgegevens verwerken om deze te verstrekken aan een orgaan in verband met diens publiekrechtelijke taak, zoals het bevoegde orgaan voor inspectie (de onderwijsinspectie). In dit kader zullen wij ook een gedegen administratie moeten voeren.

Met wie kunnen wij persoonsgegevens delen?

Wij kunnen uw persoonsgegevens in beperkte gevallen delen met derden. Dit doen wij alleen wanneer dit noodzakelijk is voor de doeleinden zoals beschreven in dit Privacy-statement, meer in het bijzonder het verzorgen van onderwijs en het bewaken van de kwaliteit van het onderwijs.

Stichting voor christelijk onderwijs Harderwijk-Hierden

Wij kunnen (als school) gegevens over uw kind delen met VCO. Wij bepalen zelfstandig onze koers terwijl VCO voor ons kwaliteitsindicatoren vaststelt om onze leerlingen zo goed mogelijk te begeleiden. Daarnaast heeft VCO bepaalde protocollen voor alle aangesloten twaalf scholen vastgesteld, bijvoorbeeld ten aanzien van de klachtenprocedures.

Ten behoeve van continuïteit en kwaliteit van het onderwijs dat wij verzorgen hebben daartoe geautoriseerde medewerkers van VCO toegang tot bepaalde administratie systemen waarin persoonsgegevens van leerlingen en hun ouders zijn vastgelegd en kunnen wij persoonsgegevens aan VCO doorgeven. In dit verband koopt VCO centraal administratieve systemen in zoals ParnasSys (leerlingen administratie en leerling volgsysteem) en OSO (Overstapservice Onderwijs dragen scholen het OSO-dossier digitaal veilig en snel over. De privacy van leerlingen is daarmee meteen goed geregeld.

VCO en de school kan centraal digitale administratiesystemen en leermiddelen inkopen, waarvan de aangesloten scholen gebruik (kunnen) maken. VCO heeft in dat geval toegang tot bepaalde persoonsgegevens om de kwaliteit van de leermiddelen te waarborgen. VCO kan voorts persoonsgegevens verwerken om het plaatsingsbeleid te optimaliseren en om vragen en klachten af te handelen.

Overheidsinstanties

Wij kunnen de persoonsgegevens van uw kind delen met overheidsinstanties, voor zover dit noodzakelijk is voor de uitoefening van een taak van algemeen belang of in verband met een wettelijke verplichting. Het kan dan bijvoorbeeld gaan om gegevens die wij verplicht zijn om te delen met bevoegde instanties, zoals de onderwijsinspectie, de Dienst Uitvoering Onderwijs (DUO) of de GGD. Ook moeten wij persoonsgegevens van uw kind delen wanneer hij of zij naar een andere school gaat – deze zijn vastgelegd in het onderwijskundig rapport. Bij een vermoeden van huishoudelijk geweld kunnen wij een melding doen bij Veilig Thuis of een andere daartoe aangewezen en bevoegde instantie. De ontvangende overheidsinstantie is zelfstandig verwerkingsverantwoordelijke en moet zich houden aan de toepasselijke privacy verplichtingen.

Externe leveranciers

Wij maken gebruik van een aantal diensten van derden om het onderwijs te ondersteunen en die als verwerker persoonsgegevens van u en/of uw kind verwerken. Wij en/of VCO hebben bijvoorbeeld afspraken gemaakt met externe leveranciers voor administratiesystemen en leerlingvolgsystemen, zoals ParnasSys.

Daarnaast maken wij gebruik van digitale leermiddelen, die wij onder andere aanbieden via de portal van Stichting Basispoort. Een overzicht van de door ons gebuikte digitale leermiddelen kunt u opvragen via de schooldirecteur. Als u wilt weten hoe de leveranciers van digitale leermiddelen omgaan met leerling gegevens, dan kunt u dat nalezen in de privacy bijsluiters die horen bij de leermiddelen die wij op school gebruiken.

Bibliotheek (is niet voor alle scholen van toepassing)

Ter ondersteuning van het onderwijs kunt u ervoor kiezen om uw kind via ons in te schrijven bij de Bibliotheek Noordwest Veluwe. Dit is niet verplicht. Wij vragen uw toestemming om persoonsgegevens zoals naam, groep en huisadres door te geven aan Bibliotheek Noordwest Veluwe. Bibliotheek Noordwest Veluwe verwerkt deze persoonsgegevens als verwerkingsverantwoordelijke voor haar eigen doeleinden en moet zelfstandig de op haar rustende privacy verplichtingen naleven.

Andere ouders

Wanneer u daarmee akkoord bent gegaan, kunnen wij voorts uw persoonsgegevens en die van uw kind delen met andere ouders, bijvoorbeeld via de klassenlijst of via online communicatie netwerken (zoals Whatsappgroepen, Facebook pagina, Klasboard, Parro of de website).
Wij hebben geen zeggenschap over de verdere verwerking van uw persoonsgegevens door derden die kennis nemen van de klassenlijst of via genoemde communicatienetwerken.

Wanneer wij persoonsgegevens delen met derden, zullen deze persoonsgegevens niet buiten de Europese Economische Ruimte worden verwerkt, tenzij hiervoor aanvullende afspraken zijn gemaakt met deze derden, of wanneer maatregelen zijn genomen die ervoor zorgen dat de privacy van u en uw kind zijn gewaarborgd.

Zijn uw persoonsgegevens veilig?

Wij hebben verschillende passende technische en organisatorische beveiligingsmaatregelen genomen om de persoonsgegevens die wij van u en uw kind verwerken te beschermen tegen verlies of onrechtmatig gebruik. Zo beveiligen wij onze systemen en applicaties volgens de geldende standaarden voor informatiebeveiliging. Wij hebben ook met leveranciers van (onder andere) onze administratiesystemen en leerlingvolgsystemen afspraken gemaakt en hen verplicht om adequate beveiligingsmaatregelen te nemen.

Hoe lang bewaren wij persoonsgegevens van u en uw kind?

Wij bewaren persoonsgegevens alleen voor zolang dit noodzakelijk is voor de doeleinden genoemd in dit Privacy-statement. In beginsel bewaren wij persoonsgegevens van u en uw kind die in het leerlingendossier zijn opgenomen tot twee jaar nadat uw kind van school is. Het is mogelijk dat wij bepaalde persoonsgegevens langer dan twee jaar bewaren, bijvoorbeeld wanneer dat wettelijk verplicht is of wanneer dat noodzakelijk is om uw en/of onze rechten te beschermen. Wij bewaren in verband met de wettelijke verplichtingen die op ons rusten de gegevens uit de verzuimadministratie minimaal vijf jaar.

Verzoeken om inzage, correctie en verwijdering

Iedere betrokkene kan op basis van de wet bepaalde rechten uitoefenen ten aanzien van zijn of haar persoonsgegevens. Zo hebt u het recht tot inzage, rectificatie en verwijdering van persoonsgegevens die op u betrekking hebben. Deze rechten kunt u ook uitoefenen namens uw kind. Ook kunt u bezwaar maken tegen het gebruik van de gegevens van uzelf of van uw kind of vragen dit gebruik te beperken. Wanneer u uw rechten uitoefent, kunt u uw verzoek sturen aan het contactadres onderaan dit Privacy-statement of aan de betreffende school. Geef daarbij duidelijk aan welke persoonsgegevens u wilt inzien, corrigeren of aanvullen.

Klachten

Als u klachten hebt over hoe wij met uw persoonsgegevens omgaan, dan kunt u contact met ons opnemen via de gegevens zoals vermeld onder 'Contact' op de schoolsite of u kunt direct contact opnemen met de Privacy officer of de Functionaris Gegevensbescherming van VCO .
Wij helpen u graag met het vinden van een oplossing. Indien dat toch niet zou lukken, dan kunt u zich altijd wenden tot de Autoriteit Persoonsgegevens.

Aanpassingen

Ontwikkelingen gaan snel en daardoor kan er soms ook iets veranderen in de persoonsgegevens die wij van u vragen en de wijze waarop wij persoonsgegevens verwerken. Ook kan regelgeving wijzigen. Wij passen daarom van tijd tot tijd ons Privacy-statement aan en raden u aan om dit regelmatig te raadplegen.

Privacy officer VCO

Dhr. Martin van den Bor: avg@stichtingvco.nl of op telefoonnummer 0341-431479

Stichting VCO beschikt ook over een Functionaris Gegevensbescherming (FG). Deze is extern belegd. Voor meer informatie zie hoofdstuk Functionaris Gegevensbescherming.

Rechten van betrokkenen

1. Basisvoorwaarden

Inleiding

De AVG geeft betrokkenen verschillende rechten ten aanzien van haar of zijn gegevens wanneer deze verwerkt worden door organisaties.[1] Dit zijn:

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

Betrokkenen kunnen op meerdere manieren een verzoek indienen: digitaal, schriftelijk of mondeling. Organisaties zijn verplicht om binnen één maand te reageren op dit verzoek. Hiervoor bestaan meerdere processen binnen VCO, om zo goed mogelijk en tijdig te voldoen aan een verzoek van een betrokkene.

Alle verzoeken van betrokkenen worden binnen 30 dagen afgehandeld. De IBP'er rapporteert jaarlijks over aantallen, doorlooptijden en eventuele overschrijdingen aan het bestuur.

Te regelen processen

De hieronder beschreven werkprocessen dragen bij aan een soepele omgang met het uitoefeningsverzoeken.

1. Faciliteren in de uitoefening van uitoefeningsverzoeken

   Een duidelijk omschreven proces voor verzoeken van betrokkenen zorgt dat betrokkenen weten hoe zij hun recht kunnen uitoefenen, en daarnaast is het duidelijk voor het personeel hoe zij met deze verzoeken moeten omgaan. In hoofdstuk 2 wordt hier meer over geschreven.

2. Motief onderzoeken van uitoefeningsverzoek

   VCO mag geen afbreuk doen aan uitoefeningsverzoeken door deze onredelijk te vertragen of te verhinderen. Wel kan het nuttig zijn om in sommige gevallen (vrijblijvend) naar het motief achter een uitoefeningsverzoek te vragen. Het motief kan duidelijkheid verschaffen over de redenen waarom een betrokkene bijvoorbeeld inzage wil krijgen. De betrokkene wordt hierdoor gemotiveerd het verzoek nader te onderbouwen, zodat de reikwijdte van diens verzoek duidelijker vastgesteld kan worden. Dit maakt de uitvoering van het uitoefeningsverzoek efficiënter. Ook kan gemakkelijker worden meegedacht met de betrokkene en worden onnodige stappen voorkomen bij de afhandeling van het verzoek.

[1] Deze rechten worden verder toegelicht in Bijlage 1: "Toelichting begrippen".

Voor meer informatie over de reikwijdte van uitoefeningsverzoeken en rechten van betrokkenen, zie de website van de Autoriteit Persoonsgegevens.

3. Aanstelling van een sleutelpersoon die regie houdt

Bij de behandeling van een uitoefeningsverzoek moet soms veel worden geschakeld met diverse afdelingen binnen VCO. In sommige gevallen zelfs buiten VCO. Om te voorkomen dat de reactietermijn op een verzoek overschreden wordt, is één medewerker aangesteld als sleutelpersoon voor de afhandeling van uitoefeningsverzoeken. Binnen VCO is dit de Privacy Officer, Martin van den Bor. Door het uitoefeningsverzoek te registreren in het register uitoefeningsverzoeken is de Privacy Officer snel op de hoogte van het uitoefeningsverzoek, zodat de termijn van één maand niet uit het oog wordt verloren. Door nauwkeurige opvolging van uitoefeningsverzoeken, krijgt de Privacy Officer inzage in wat de status is van een uitoefeningsverzoek en welke acties open staan.
Indien de Functionaris Gegevensbescherming (FG) van VCO een verzoek van betrokkene ontvangt, dan zal de reikwijdte van het verzoek vastgesteld worden en gedeeld worden met de Privacy Officer.

4. Verzameling van de data in een centraal systeem

Een uniforme behandeling van uitoefeningsverzoeken zorgt ervoor dat de verzameling van de verzochte gegevens zo min mogelijk tijd kost. Het uitoefeningsverzoekenregister draagt hieraan bij omdat het een volledig inzicht geeft in alle gegevens van de betrokkene. Als dit niet aanwezig is, dan is het belangrijk om inzichtelijk te maken waar de gegevens zich in welke processen bevinden. Het register van verwerkingsactiviteiten ondersteunt dit. Indien nodig wordt contact opgenomen met andere/externe partijen om de relevante gegevens op te vragen. Ook draagt een centrale verzameling van uitoefeningsverzoeken in het register bij aan een gemakkelijke vastlegging van de identiteit van de verzoeker door de sleutelpersoon. Dit is noodzakelijk, zodat de verzochte data enkel aan de juiste persoon verstuurd wordt.

5. Aanpassing van de verzamelde data indien nodig voor uitgave

Indien de verzamelde data informatie bevat over derden, óf wanneer de informatie niet bijdraagt aan het doel van het verzoek, dan moet de data aangepast worden voordat deze gedeeld wordt. Denk hierbij aan het afschermen van mailadressen van derden, of het redigeren van gevoelige gegevens. Overleg bij twijfelgevallen over de gevoeligheid van informatie met de privacy-coördinator en/of de ICT afdeling om de noodzaak van aanpassing van deze informatie te beoordelen.

6. Verzamelen van de data in één bestand en begeleidende tekst

Afhankelijk van het verzoek moet er informatie worden gewijzigd, aangeleverd of verwijderd. Is de juiste informatie verzameld, dan wordt dit aangeleverd in één bestand en in één reactie aan de verzoeker. In de reactie staat wat de inhoud van deze informatie is en wordt eventueel een toelichting gegeven waarom bepaalde informatie is geredigeerd of in aangepaste vorm is gedeeld. In uitzonderlijke gevallen kan het zijn dat het verzamelen van de gegevens langer duurt dan één maand. De verzoeker wordt in dit geval geïnformeerd waarbij verplicht uitgelegd wordt waarom de reactietermijn wordt verlengd.

7. Keuze voor communicatiekanaal

Bij de keuze van de manier waarop gecommuniceerd wordt over het verzoek, moet rekening worden gehouden met de mate van noodzakelijke (informatie)beveiliging, en met het door de verzoeker gewenste communicatiekanaal voor ontvangst van de verzochte informatie. De communicatie van bijzondere persoonsgegevens, zoals bijvoorbeeld het medisch dossier, moet beter beveiligd worden voor de (digitale) verzending dan wanneer verzocht is om NAW-gegevens. Het communicatiekanaal dat gebruikt is door de verzoeker hoeft niet het communicatiekanaal te zijn dat gebruikt wordt voor de verzending van de verzochte informatie. Stem dit af met de verzoeker.

8. Bijhouden register met verzoeken

Alle uitoefeningsverzoeken worden bijgehouden in het uitoefeningsverzoekenregister zodat eenieder de voortgang van een verzoek kan volgen en extra informatie kan aanleveren waar nodig. Voor de aantoonbaarheid van behandelde uitoefeningsverzoeken bevat het register de bronnen van alle verzamelde informatie, de beoordelingsstappen en de beslissingen omtrent eventuele uitzonderingen en de verstrekte antwoorden.
Het periodieke organisatieverslag bevat een samenvatting van het uitoefeningsverzoekenregister. Hierbij wordt gerapporteerd over de aantallen, de aard van de verzoeken en de mate waarin deze binnen de wettelijke termijnen zijn afgehandeld, conform de vastlegging in het register zoals beschreven in het Privacyreglement.

2. Protocol afhandelen van een verzoek inzake rechten van betrokkenen

Zodra een betrokkene een verzoek indient bij VCO, dan komt dit verzoek terecht bij de Privacy Officer, Martin van den Bor. Beoordeeld wordt om wat voor soort verzoek het gaat en de FG kan hierbij geraadpleegd worden indien nodig. Nadat vast is gesteld om wat voor een verzoek het gaat, wordt overgegaan tot de benodigde acties om het verzoek te behandelen.
Zoals gecommuniceerd in de privacyverklaring, wordt een verzoek van betrokkene bij voorkeur ingediend per mail of post bij VCO.
Als een verzoek op een andere wijze binnenkomt, dan wordt de Privacy Officer ingelicht en wordt het verzoek vastgelegd in het register.

Stap 1: ontvangst verzoek van betrokkene

Ontvangst door: [naam persoon]
Tijdsindicatie: 0 – 30 minuten

- Bevestig de ontvangst van het verzoek via hetzelfde communicatiekanaal wat gebruikt is voor het indienen van het verzoek door de betrokkene;
- Geef in de bevestiging weer dat een inhoudelijke reactie binnen één maand volgt.

Stap 2: vastlegging en beoordeling verzoek en identificatie betrokkene

Vastlegging en beoordeling door: [naam persoon]
Tijdsindicatie: 30 – 60 minuten

- Datum van ontvangst verzoek vastleggen;
- Identiteit van verzoeker verifiëren;

- De identiteit moet worden vastgesteld van de verzoeker voordat het uitoefeningsverzoek in behandeling wordt genomen. Dit is noodzakelijk om te voorkomen dat bijvoorbeeld de persoonsgegevens naar iemand anders worden geopenbaard of van de verkeerde persoon gegevens worden verwijderd. De controle op de identiteit moet strenger worden toegepast wanneer de aard van de persoonsgegevens gevoelig of bijzonder is. Het vragen van een kopie legitimatiebewijs om de identiteit van de verzoeker vast te stellen is daarbij ongewenst: hiervoor bestaan minder ingrijpende manieren, zie de site van de AP.

- Beoordelen of er sprake is van een wettelijk verbod op inzage (of een ander recht van betrokkene) waardoor het verzoek niet (volledig) ingewilligd kan worden; Zie voor toelichting bijlage 1.
- Controleren of er sprake is van een bijzondere omstandigheid met betrekking tot het uitoefeningsverzoek. Denk hierbij aan gevallen waarbij het verzoek van de betrokkene niet ingewilligd hoeft te worden; Zie voor toelichting bijlage 1.
- Stel vast wie of wat nodig is voor het uitvoeren van het verzoek. Bepaal waar gezocht moet worden, wat verzameld/gewijzigd/verwijderd moet worden en wie hiervoor nodig is. Raadpleeg hiervoor indien nodig de beheerder(s) van de applicatie(s) waar de persoonsgegevens van de betrokkene mogelijk in staan.

Stap 3: Verzameling (persoons)gegevens	
Verzameling door:	[beheerder: naam persoon]
Tijdsindicatie:	niet langer dan 15 dagen

Afhankelijk van hetgeen waar naar verzocht wordt, zijn de antwoorden op de volgende vragen een leidraad voor de behandeling van een verzoek tot inzage in de persoonsgegevens die VCO verwerkt:

- Welke persoonsgegevens worden verwerkt?
- Wat zijn de verwerkingsdoeleinden?
- Wie zijn de ontvangers van de persoonsgegevens?
- Wat zijn de (gebruikte) bewaartermijnen?
- Wat is de bron van de persoonsgegevens wanneer deze gegevens niet van de betrokkene zelf komen?
- Worden de persoonsgegevens verwerkt op geautomatiseerde wijze (“profiling”)? Indien dit het geval is, welke persoonsgegevens worden hiervoor gebruikt en wat wordt hiermee gedaan?

Let op: indien [naam persoon stap 2] geen reactie heeft ontvangen na 10 dagen van de beheerder(s), dan wordt er een herinnering verstuurd naar de beheerder in kwestie.

Stap 4: (concept) reactie op verzoek formuleren	
Opstelling reactie door:	[naam persoon]
Tijdsindicatie:	twee dagen

Nadat alle informatie is verzameld of wanneer het verzoek (intern) is afgehandeld wordt er een inhoudelijke reactie opgesteld richting de betrokkene. De reactie wordt uiteindelijk via hetzelfde kanaal als waarop het verzoek is binnengekomen verstuurd richting de betrokkene.
Vervolgens wordt er een keuze gemaakt tussen het maken van volledige kopieën of van alleen de gebruikte persoonsgegevens, als het een inzageverzoek betreft.
Aandachtspunten voor de inhoudelijke reactie:

- Geen tijdige reactie (binnen één maand): Indien de ingewikkeldheid en/of het aantal verzoeken het niet toelaten om binnen één maand te reageren, dan kan de reactietermijn met twee maanden worden verlengd. Hierover wordt betrokkene binnen één maand na ontvangst geïnformeerd , voorzien van een onderbouwing van het uitstel.
- Weigering: de weigering van een verzoek wordt uitgelegd aan de verzoeker.
- Mogelijkheid voor het indienen van een klacht: in de reactie wordt de betrokkene er altijd van in kennis gesteld dat zij of hij de mogelijkheid heeft om een klacht in te dienen bij de AP als hij/zij niet tevreden is met de reactie.

Stap 5: Registreren van verzoeken en de in-/aanvulling hiervan nadat verzoek is afgehandeld

Opstelling reactie door: [naam persoon]
Tijdsindicatie: één dag
Nadat het uitoefeningsverzoek van de betrokkene volledig is afgehandeld wordt gecontroleerd of alles is vastgelegd in het uitoefeningsregister. Vermeld ook dat het verzoek is afgehandeld.

Bijlage 1: Toelichting begrippen

Deze bijlage geeft de (juridische) achtergrond weer bij de stappen die genomen moeten worden wanneer betrokkenen hun rechten uit de AVG wensen uit te oefenen met betrekking tot de door organisaties verwerkte persoonsgegevens.

1. Behandeling verzoek om inzage

   De betrokkene heeft het recht om te weten of haar of zijn persoonsgegevens verwerkt worden door organisaties. Indien dit het geval is, dan heeft zij of hij het recht om inzage te krijgen in die persoonsgegevens en in de volgende informatie met betrekking tot diens persoonsgegevens:[2]

   A. De verwerkingsdoeleinden;
   B. De betrokken categorieën van persoonsgegevens;
   C. De ontvangers of categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt, met name ontvangers in derde landen of internationale organisaties;
   D. Wanneer persoonsgegevens doorgegeven worden aan een derde land of een internationale organisatie: informatie over de passende (privacy-)waarborgen in dat derde land (overeenkomstig artikel 46 van de Avg);
   E. Indien mogelijk, de periode gedurende welke de persoonsgegevens naar verwachting opgeslagen zullen worden, of indien dit niet mogelijk is, de criteria om die termijn te bepalen;
   F. Wanneer de persoonsgegevens niet bij de betrokkene verzameld worden, alle beschikbare informatie over de bron van die gegevens;

[2] Artikel 15 AVG.

G. Het bestaan van geautomatiseerde besluitvorming, waaronder profiling (zie artikel 22 van de Avg), en, ten minste in die gevallen, nuttige informatie over de onderliggende logica, het belang en de verwachte gevolgen van die verwerking voor de betrokkene;
H. Een kopie van de persoonsgegevens die verwerkt worden. Wanneer de betrokkene zijn verzoek elektronisch indient, en niet om een andere regeling (bijvoorbeeld papier) verzoekt, wordt de informatie in een gangbare elektronische vorm verstrekt.

Beperkingen verzoek om inzage
Een inzage verzoek mag geen afbreuk doen aan de rechten en vrijheden van anderen.[3] Dit betekent dat het recht op inzage van een betrokkene niet onbeperkt is in de uitvoering hiervan. Bij de verstrekking van de verzochte gegevens mogen de rechten en vrijheden van anderen niet in het gedrang komen. Zo kunnen "interne stukken" zoals vastleggingen van besproken punten tijdens een overleg niet zonder meer ingezien worden wanneer een betrokkene een inzageverzoek doet in deze stukken. Dit kan namelijk afbreuk doen aan de rechten en vrijheden van anderen wanneer persoonlijke meningen en gedachten van anderen over betrokkene tijdens een overleg zijn geuit en vastgelegd. Dergelijke uitingen en meningen vallen dus onder de bescherming van rechten en vrijheden van anderen. De uitwerking van een overleg in "interne stukken" daarentegen mogen wel ingezien worden vanwege het ontbreken van persoonlijke gedachten van individuen.
Verder mag een verzoek tot inzage niet oneigenlijk gebruikt worden. Wanneer een verzoek om inzage kennelijk oneigenlijk wordt gebruikt, dan hoeft dit niet gehonoreerd te worden. Voor een dergelijke afwijzing moet wel voldoende aannemelijk zijn dat er misbruik wordt gemaakt van het recht.
Hierbij kan gedacht worden aan het verzamelen van informatie voor andere doeleinden anders dan het controleren van de rechtmatigheid van de verwerking van de persoonsgegevens.

Aandachtspunt bij de behandeling van het verzoek om inzage:
In gevallen waarbij de verzamelde informatiegegevens bevat over derden of wanneer de onthulling van informatie niet bijdraagt aan het doel van het verzoek van betrokkene, dan dient de verzamelde informatie in aangepaste wijze gedeeld te worden met betrokkene. Denk hierbij aan het afschermen van mailadressen van derden wanneer mailcorrespondentie wordt gedeeld met de betrokkene of het redigeren van gevoelige gegevens in de aantekeningen van een medewerker in een dossier van de betrokkene. Hierbij moet dus rekening gehouden worden met het (privacy)belang van die derde door die gegevens van derden te verwijderen of aan te passen, of pas na toestemming van die derde de gegevens te verstrekken. [4]
Overleg in gevallen waarbij twijfel bestaat over de gevoeligheid van informatie met de privacy coördinator en de ICT-afdeling om de noodzaak van aanpassing van deze informatie te beoordelen.

2. <u>Behandeling verzoek om aanpassing of verwijdering persoonsgegevens</u>

[3] Artikel 14 lid 4 AVG; artikel 23 lid 1 (i) AVG.
[4] Artikel 14 lid 4 AVG; artikel 23 lid 1 (i) AVG.

De betrokkene heeft het recht om haar of zijn persoonsgegevens die verwerkt worden aan te laten passen of te laten verwijderen, omdat deze bijvoorbeeld onjuist blijken te zijn nadat deze zijn ingezien door de betrokkene.[5]

Rectificatieverzoek

Een verzoek om aanpassing van persoonsgegevens van betrokkene ("rectificatieverzoek") betreft de aanpassing van de persoonsgegevens zoals deze zijn opgenomen binnen VCO. Een verzoek van een betrokkene om diens persoonsgegevens aan te laten passen kan óók gaan om een aanvulling van ontbrekende gegevens of de toevoeging van een verklaring. Het laatste kan zich voordoen indien de betrokkene een andere opvatting heeft over de persoonsgegevens zoals die op dat moment verwerkt worden door VCO. Denk hierbij aan een negatieve beoordeling of berisping waar de betrokkene een andere opvatting over heeft en haar of zijn eigen verklaring wil laten toevoegen aan het dossier.

Verwijderingsverzoek

Een betrokkene heeft het recht om van organisaties te verwachten dat diens persoonsgegevens zonder onredelijke vertraging wordt verwijderd indien hier om wordt verzocht. VCO is verplicht om een verwijderingsverzoek in te willigen zonder onredelijke vertraging indien sprake is van één van de volgende gevallen:[6]

- De persoonsgegevens zijn niet langer nodig voor de doeleinden waarvoor zij verzameld of anderszins verwerkt zijn;
- De betrokkene trekt de eerder gegeven toestemming in en er is geen andere rechtsgrond voor de verwerking. De betrokkene moet zijn toestemming op dezelfde manier kunnen intrekken als dat hij hem gegeven heeft;
- De betrokkene maakt bezwaar tegen de verwerking en er zijn geen andere dwingende gerechtvaardigde gronden voor de verwerking.[7] Let op: dit dwingt de VCO tot een belangenafweging. Zie voor meer informatie hierover punt 4 in deze toelichting 'Behandeling indiening bezwaar tegen verwerking persoonsgegevens'
- De persoonsgegevens zijn onrechtmatig verwerkt;
- De persoonsgegevens moeten worden verwijderd om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust.

In de volgende gevallen hoeft het verzoek van de betrokkene niet ingewilligd te worden:

- Voor het uitoefenen van het recht op vrijheid van meningsuiting en informatie (denk aan journalistiek, nieuwssites of archieven);
- Voor het nakomen van een wettelijke verwerkingsverplichting die op VCO rust. In de HR-bestanden zitten bijvoorbeeld bepaalde gegevens van werknemers die verstrekt moeten worden aan de Belastingdienst;
- Met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek;
- Voor de instelling, uitoefening of onderbouwing van een rechtsvordering.

[5] Artikel 16 AVG; artikel 17 AVG.
[6] Artikel 17 lid 1 AVG.
[7] Artikel 21 AVG.

3. Verzoek om beperking van verwerking persoonsgegevens

Een betrokkene heeft het recht om de verwerking van diens persoonsgegevens (tijdelijk) te laten beperken in de volgende gevallen:[8]

- Bij betwisting van de juistheid van de persoonsgegevens door de betrokkene, gedurende een periode die VCO in staat stelt de juistheid van de persoonsgegevens te controleren;
- De verwerking is onrechtmatig en de betrokkene verzet zich tegen het verwijderen van de persoonsgegevens, maar in de plaats daarvan verzoekt hij om beperking van het gebruik ervan;
- VCO heeft de persoonsgegevens niet meer nodig voor de verwerkingsdoeleinden, maar de betrokkene heeft deze nodig voor de instelling, uitoefening of onderbouwing van een rechtsvordering;
- De betrokkene heeft bezwaar gemaakt tegen de verwerking, in afwachting van het antwoord op de vraag of de gerechtvaardigde gronden van VCO zwaarder wegen dan die van de betrokkene.

Afhandeling verzoek om rectificatie, verwijdering of beperking

Het rectificatie- en/of verwijderingsverzoek dient binnen één maand behandeld te worden en de betrokkene dient zo snel mogelijk op de hoogte gesteld te worden over de inwilliging van diens verzoek.[9] Als het verzoek niet ingewilligd wordt, dan dient de reden hiertoe gemotiveerd aangegeven te worden. Als het verzoek wel ingewilligd wordt, dan dient dit gedeeld te worden met de betrokkene. Hierbij moeten eventuele ontvangers van de persoonsgegevens van de betrokkenen (bijvoorbeeld extern administratiekantoor) óók op de hoogte gebracht worden over de rectificatie, verwijdering of beperking van verwerkingen zodat zij ook de rectificatie, verwijdering of beperking doorvoeren.

4. Behandeling indiening bezwaar tegen verwerking persoonsgegevens

Een betrokkene heeft altijd het recht om een bezwaar in te dienen tegen de verwerking van diens persoonsgegevens indien hiervoor het gerechtvaardigd belang of de taak van algemeen belang als verwerkingsgrondslag wordt gebruikt. Dit bezwaar dient dan wél omkleed te worden met redenen die verband houden met de specifieke situatie van betrokkene.[10]
Indien VCO geen dwingende gerechtvaardigde gronden kan aanvoeren voor de verwerking die zwaarder wegen dan de belangen, rechten en vrijheden van de betrokkene, dan moet VCO de verwerking te staken. Dit geldt ook wanneer er niet aangetoond kan worden dat de verwerking verband houdt met de instelling, uitoefening of onderbouwing van een rechtsvordering.

In het geval dat een betrokkene een met redenen omkleed bezwaar indient tegen de verwerking van diens persoonsgegevens dat verband houdt met haar of zijn specifieke geval, dan zal VCO een belangenafweging moeten maken. Bij deze belangenafweging dient bezien te worden of het belang van de betrokkene in een specifiek geval zwaarder weegt dan het belang van VCO.

[8] Artikel 18 lid 1 AVG.
[9] Artikel 12 lid 3 AVG.
[10] Artikel 21 AVG.

5. Behandeling verzoek tot dataportabiliteit

Een betrokkene heeft het recht om gegevens mee te nemen van de ene organisatie naar een andere organisatie.[11] Zo mag een leerling haar of zijn persoonsgegevens opvragen bij de oude school, verzoeken dat deze persoonsgegevens verwijderd worden en de verkregen persoonsgegevens aanreiken aan de nieuwe school. Dit heet het recht op dataportabiliteit. Een betrokkene kan een dergelijk verzoek enkel doen ten aanzien van diens eigen gegevens die zij of hij zélf heeft verstrekt. Een betrokkene kan diens gegevens opvragen indien de verwerking berust op de verwerkingsgrondslag 'toestemming' of 'uitvoering van een overeenkomst', en indien de verwerking via geautomatiseerde wijze verloopt.

De verstrekking van de verzochte data moet op een gestructureerd, gangbare en op een machine leesbare vorm plaatsvinden zodat de betrokkene zelf of de door de betrokkene gekozen organisatie deze data verder kan verwerken. De data moet dus toegankelijk zijn voor de betrokkene en/of de organisatie waarvoor het is bestemd.

6. Wijze van antwoorden

De inhoudelijke reactie van VCO op het verzoek van betrokkene dient binnen de door de AVG gestelde termijn van één maand voorzien te worden.[12] Afhankelijk van de ingewikkeldheid en aantal verzoeken, kan de reactietermijn met twee maanden worden verlengd.[13] Ook hierover zal de betrokkene zo snel mogelijk geïnformeerd worden (in ieder geval binnen één maand na ontvangst van het verzoek), voorzien van een onderbouwing.
De reactie dient te geschieden op dezelfde wijze als waarop het verzoek is binnengekomen. Dit betekent dat een inzageverzoek dat per post is ingediend ook per brief beantwoord dient te worden. Hetzelfde geldt voor verzoeken die elektronisch ingediend worden. De reactie dient in een gangbaar formaat aangeleverd te worden aan de betrokkene. Inzage is kosteloos. Wel mag er voor extra kopieën een redelijke vergoeding gevraagd worden. Hierbij worden de richtlijnen die worden opgesteld door de Autoriteit Persoonsgegevens (AP) gevolgd zoals deze hier te raadplegen zijn.

7. Mogelijkheid tot het indienen van een klacht bij VCO of bij de Autoriteit Persoonsgegevens

Tot de rechten van de betrokkene behoort ook de mogelijkheid om een klacht in te dienen bij de VCO zelf of bij de Autoriteit Persoonsgegevens wanneer de betrokkene niet tevreden is met de inhoudelijke reactie. In de inhoudelijk reactie moet daarom altijd de mogelijkheid voor de betrokkene om een klacht in te dienen bij VCO en bij de Autoriteit Persoonsgegevens, benoemd worden.

[11] Artikel 20 AVG.
[12] Artikel 12 lid 3 AVG.
[13] Artikel 12 lid 3 AVG.

1	Nummer/referentie uitoefeningsverzoek	1	Nummer/referentie uitoefeningsverzoek	1	Nummer/referentie uitoefeningsverzoek
	Verzoek doorgevoerd bij de		Identificatie verzoeker vastgesteld		Naam verzoeker
	Verzoek afgehandeld		Korte omschrijving verzoek		Optioneel: Reden van verzoek
	Afhandelingsdatum		Bijzondere omstandigheden verzoek		Soort verzoek
			Gebruik van profiling (verwerking op geautomatiseerde wijze)		Naam behandelaar
	Afhandelingsduur		Vervolg onderzoek Ja/nee Omschrijving		FG betrokken
	Reactie betrokkene		Inwilliging verzoek mogelijk?		Medium ontvangst verzoek (digitaal/post)
	Evaluatieverzoek (wat is gedaan)		Motivatie afwijzing van verzoek (indien van toepassing)		Datum ontvangst verzoek
			Verlenging maximale termijn nodig?		Ontvangst verzoek bevestigd
	Documenten in map (bewijsstukken i.e. reactie richting		Motivatie verlenging termijn		Deadline oplevering

Recht op vergetelheid

In de Algemene Verordening Gegevensbescherming (AVG) is het recht op vergetelheid opgenomen. Dit recht houdt in dat in een aantal gevallen iemands persoonsgegevens moeten worden gewist. Ouder(s)/verzorger(s), personeel en personen buiten de organisatie kunnen aan VCO vragen om hun gegevens te wissen met een beroep op hun recht op vergetelheid.

Wanneer geldt het recht op vergetelheid?

In de volgende situaties moet VCO iemands persoonsgegevens wissen:

- *Niet meer nodig*
  VCO heeft de persoonsgegevens niet meer nodig voor de doeleinden waarvoor VCO ze heeft verzameld of waarvoor VCO verwerkt.
- *Toestemming ingetrokken*
  De betrokkene heeft eerder (uitdrukkelijke) toestemming gegeven aan VCO voor het gebruik van zijn gegevens, maar trekt die toestemming nu in.
- *Bezwaar*
  De betrokkene maakt bezwaar tegen de verwerking. Er geldt op grond van artikel 21 van de AVG een absoluut recht van bezwaar tegen direct marketing. Een relatief recht van bezwaar geldt als de rechten van de betrokkene zwaarder wegen dan het belang van VCO om de persoonsgegevens te verwerken.
- *Onrechtmatige verwerking*
  VCO verwerkt de persoonsgegevens onrechtmatig. Bijvoorbeeld omdat er geen wettelijke grondslag is voor de verwerking.
- *Wettelijk bepaalde bewaartermijn verlopen*
  VCO is wettelijk verplicht om de gegevens na bepaalde tijd te wissen.
- *Apps en websites bij kinderen*
  De betrokkene is jonger dan 16 jaar en de persoonsgegevens zijn verzameld via een app of website (‘dienst van de informatiemaatschappij’).

Wanneer geldt het recht op vergetelheid niet?

Er is een aantal uitzonderingen op het recht op vergetelheid.
Bijvoorbeeld als VCO wettelijk verplicht is om bepaalde gegevens te verwerken. Dan kan VCO deze gegevens niet op verzoek wissen. Het recht op vergetelheid is in principe niet namens iemand anders op te eisen, tenzij u daar bijvoorbeeld een volmacht voor heeft.
Vraagt iemand op grond van het recht op vergetelheid om zijn gegevens te wissen, dan moet VCO daar onmiddellijk gehoor aan geven, en wel uiterlijk binnen een maand. Alleen als het om een heel complex verzoek gaat, is twee maanden extra de tijd beschikbaar. VCO moet binnen een maand aan de betrokkene laten weten dat de periode verlengd wordt.

Manier van reageren

Als een betrokkene het verzoek elektronisch indient, moet VCO ook elektronisch reageren, tenzij de betrokkene ons vraagt om op een andere manier te reageren.

Kosten
VCO mag in principe géén kosten berekenen voor het wissen van persoonsgegevens. Alleen indien VCO kan bewijzen dat een verzoek ongegrond of buitensporig is (veelvuldig herhaalde verzoeken van één persoon), dan mag VCO een redelijke administratieve vergoeding vragen of het verzoek weigeren.

Derde partijen informeren
Heeft VCO de betreffende persoonsgegevens aan derde partijen verstrekt, dan moeten die ontvangers ook geïnformeerd worden dat wij deze persoonsgegevens hebben gewist (bv Perspectief) en aangeven dat ook de ontvangers iedere kopie van, of koppeling naar, die persoonsgegevens moeten wissen. Publiceert VCO bijvoorbeeld persoonsgegevens via een website? Dan moeten zij zoekmachines informeren. Zij kunnen daarbij de webpagina opnieuw laten indexeren, zodat de gewiste persoonsgegevens niet meer verschijnen in de zoekresultaten.
Als een betrokkene erom vraagt, moeten zij ook vertellen welke ontvangers zij op die manier hebben geïnformeerd (artikel 19 van de AVG).

Back-ups
Het recht op vergetelheid is ook van toepassing op digitale back-upbestanden.
Vraagt iemand VCO om zijn gegevens te wissen, dan moet VCO zijn of haar persoonsgegevens dus ook zo snel mogelijk uit uw back-ups verwijderen.

Eisen aan back-ups
Hoe op een verantwoorde manier om te gaan met back-ups onder de AVG:

- Inventariseren van welke gegevens back-ups bijgehouden moeten worden, bijvoorbeeld vanwege ons beveiligingsbeleid.
- Er rekening mee houden dat alleen gegevens mogen worden verwerkt die noodzakelijk zijn voor het doel van de verwerking (zie artikel 5 van de AVG). VCO moet kunnen aantonen dat deze gegevens noodzakelijk zijn. Dat is onderdeel van onze verantwoordingsplicht.
- Regelmatig back-ups maken en systematisch verouderde gegevens verwijderen.
- Mensen goed en duidelijk informeren over welke aanvullende bewaartermijn noodzakelijk is voor back-ups van onze specifieke dienstverlening.
- Het back-upsysteem zo inrichten in dat verwijderverzoeken van betrokkenen goed doorgevoerd kunnen worden in het systeem.

Uitzonderingen
Er zijn ook uitzonderingen op het recht op vergetelheid in back-ups. Persoonsgegevens hoeven niet uit het back-ups systeem verwijderd te worden als wettelijk verplicht is om de gegevens een bepaalde tijd te bewaren. Of als deze gegevens bewaard moeten blijven in het algemeen belang.