|  |
| --- |
|  |
|  |



**Privacyreglement Koninklijke Visio**

Juli 2021

|  |  |
| --- | --- |
| Auteur: | Functionaris Gegevenbescherming |
| Datum: | Juli 2021 |
|  |  |
|  |  |

Privacyreglement Koninklijke Visio

Juli 2021

Inhoud

[1. Inleiding 5](#_Toc45183872)

[1.1 Waarom dit privacyreglement? 5](#_Toc45183873)

[1.2 Privacywetgeving 5](#_Toc45183874)

[1.3 Voor wie is dit reglement bedoeld? 6](#_Toc45183875)

[2. Uitgangspunten verwerking Persoonsgegevens 7](#_Toc45183876)

[2.1 Verwerking van Persoonsgegevens 7](#_Toc45183877)

[2.2 Beginselen inzake persoonsgegevens verwerking 7](#_Toc45183878)

[2.3 Doeleinden bij verwerking van persoonsgegevens domein onderwijs 8](#_Toc45183879)

[3. Rechtmatige gegevensverwerking 9](#_Toc45183880)

[3.1 Voorwaarden verwerking Persoonsgegevens 9](#_Toc45183881)

[3.2 Voorwaarden voor het verwerken van gezondheidsgegevens 9](#_Toc45183882)

[3.3 Wanneer mogen andere bijzondere gegevens dan de gezondheidsgegevens worden verwerkt? 10](#_Toc45183883)

[3.4 Gegevensverwerking door een verwerker 10](#_Toc45183884)

[3.5 Gezamenlijke verwerkingsverantwoordelijken 11](#_Toc45183885)

[3.6 Aansprakelijkheid verwerkingsverantwoordelijke en/of verwerker 11](#_Toc45183886)

[4. Verstrekking van gegevens aan derden 13](#_Toc45183887)

[4.1 Geheimhoudingsplicht 13](#_Toc45183888)

[4.2 Verstrekking van cliëntgegevens aan derden 13](#_Toc45183889)

[4.2.1 Informatie uitwisseling met rechtstreeks betrokkenen 13](#_Toc45183890)

[4.2.2 Toestemming 13](#_Toc45183891)

[4.2.3 Wettelijke verplichting 14](#_Toc45183892)

[4.2.4 Conflict van plichten 14](#_Toc45183893)

[4.2.5 Meldrechten 15](#_Toc45183894)

[5. Gebruik van gegevens voor wetenschappelijk onderzoek 16](#_Toc45183895)

[5.1 Wanneer mogen gegevens aan een ander worden verstrekt voor wetenschappelijk onderzoek en statistiek op het gebied van de volksgezondheid? 16](#_Toc45183896)

[5.2 Afspraken met de onderzoeker 17](#_Toc45183897)

[6. Rechten van betrokkenen 18](#_Toc45183898)

[6.1 Voorwaarden met betrekking tot de uitvoering van de rechten van de betrokkenen 18](#_Toc45183899)

[6.2 Recht op inzage en afschrift/kopie 18](#_Toc45183900)

[6.3 Recht op informatie 20](#_Toc45183901)

[6.3.1 Te verstrekken informatie 20](#_Toc45183902)

[6.3.2 Te verstrekken informatie wanneer de persoonsgegevens niet van de betrokkene zijn verkregen 21](#_Toc45183903)

[6.3.3 Wijze van informatieverstrekking 22](#_Toc45183904)

[6.4 Recht op gegevensoverdraagbaarheid (dataportabiliteit) 22](#_Toc45183905)

[6.5 Recht op rectificatie, aanvulling en beperking van Persoonsgegevens 22](#_Toc45183906)

[6.6 Recht op gegevenswissing (recht op vergetelheid) 23](#_Toc45183907)

[6.7 Recht van bezwaar 24](#_Toc45183908)

[6.8 Vertegenwoordiging 24](#_Toc45183909)

[6.8.1 Jeugdige jonger dan 12 jaar of wilsonbekwame jeugdige van 12 tot 18 jaar 24](#_Toc45183910)

[6.8.2 Wilsbekwame cliënt van twaalf jaar of ouder 25](#_Toc45183911)

[6.8.3 Wilsonbekwame cliënt van 18 jaar en ouder 25](#_Toc45183912)

[7. Bewaartermijnen 25](#_Toc45183913)

[8. Veilige omgang met gegevens 27](#_Toc45183914)

[8.1 Verantwoordelijkheid van de verwerkingsverantwoordelijke 27](#_Toc45183915)

[8.2 Gegevensbescherming door ontwerp en standaardinstellingen (Privacy by design en default) 27](#_Toc45183916)

[8.3 Gegevensbescherming door ontwerp en standaardinstellingen bij Digitale Onderwijsmiddelen 28](#_Toc45183917)

[8.4 Gezamenlijke verwerkingsverantwoordelijken 28](#_Toc45183918)

[8.5 Register van verwerkingen 28](#_Toc45183919)

[8.6 Medewerking verlenen aan/samenwerken met de Autoriteit persoonsgegevens 29](#_Toc45183920)

[8.7 Gegevensbeschermingseffectbeoordeling (DPIA) 29](#_Toc45183921)

[8.8 Voorafgaande raadpleging van de Autoriteit Persoonsgegevens 30](#_Toc45183922)

[8.9 Beveiliging van de verwerking 31](#_Toc45183923)

[8.10 Meldplicht datalekken 32](#_Toc45183924)

[8.10.1 Melding van een inbreuk in verband met persoonsgegevens aan de Autoriteit Persoonsgegevens (datalekken melden aan de AP) en datalekkenregister 32](#_Toc45183925)

[8.10.2 Melding van een inbreuk in verband met persoonsgegevens aan de betrokkenen (datalekken melden aan de betrokkene) 33](#_Toc45183926)

[8.11 Afhandeling datalekken 34](#_Toc45183927)

[9. Functionaris voor gegevensbescherming 35](#_Toc45183928)

[9.1 Aanstelling van de functionaris voor gegevensbescherming 35](#_Toc45183929)

[9.2 Positie van de functionaris voor gegevensbescherming 35](#_Toc45183930)

[9.3 Taken van de functionaris voor gegevensverwerking 36](#_Toc45183931)

[9.4 Klachten 37](#_Toc45183932)

[10. Wijzigingen en inzage van dit reglement 38](#_Toc45183933)

[Bijlage 1 - Begripsbepalingen 39](#_Toc45183934)

[Bijlage 2 –Verwerking van persoonsgegevens onderwijs 41](#_Toc45183935)

[1. Doeleinden bij verwerking van persoonsgegevens met behulp van leermiddelen en toetsen 41](#_Toc45183936)

[2. Doeleinden bij verwerking van Persoonsgegevens met behulp van School- en Leerlinginformatiesystemen 42](#_Toc45183937)

[3. Gegevensbescherming door ontwerp en standaardinstellingen bij Digitale Onderwijsmiddelen 43](#_Toc45183938)

# Inleiding

## Waarom dit privacyreglement?

Wij, als medewerkers van Koninklijke Visio, zijn verantwoordelijk voor het beschermen van de gegevens die cliënten, cliëntvertegenwoordigers, medewerkers, leerlingen en bezoekers aan ons toevertrouwen. Koninklijke Visio neemt de bescherming van deze gegevens serieus omdat wij ook hierin een betrouwbare partner willen zijn.

In het privacybeleid staan de uitgangspunten voor privacybescherming beschreven. Het beleid bevat een aantal principes en hoofdregels die we bij Koninklijke Visio hanteren om de privacy van cliënten, leerlingen, medewerkers en ieder ander van wie wij Persoonsgegevens verwerken, te beschermen. Dit privacyreglement is een verdieping van het privacybeleid en beschrijft hoe Koninklijke Visio met de bescherming van persoonsgegevens omgaat. Dit is een uitwerking van de privacywetgeving.

## Privacywetgeving

De regels die vertellen hoe Koninklijke Visio om moet gaan met Persoonsgegevens zijn vastgelegd in verschillende wetten. In de Algemene verordening gegevensbescherming (AVG) en de Uitvoeringswet AVG (UAVG) staan de algemene regels rondom privacybescherming. Daarnaast geldt voor Koninklijke Visio sectorspecifieke wetgeving waarin regels over privacy zijn opgenomen.

Voor de zorgactiviteiten van Koninklijke Visio zijn dit onder andere de Wet op de geneeskundige behandelingsovereenkomst (Wgbo), de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (Wabvpz), het besluit elektronische verwerking door zorgaanbieders (Bevz), de Zorgverzekeringswet (Zvw), de Wet langdurige zorg (Wlz), de Wet Maatschappelijke Ondersteuning 2015 (Wmo 2015), de Jeugdwet (Jw), de wet zorg en dwang (WZD), de wet medezeggenschap cliënten zorginstellingen (WMCZ), de wet klachten kwaliteit en geschillen zorg (WKKGZ) en de wet op het Medisch-wetenschappelijk onderzoek met mensen.

Voor de onderwijsactiviteiten van Koninklijke Visio zijn dit onder meer de wet op de expertisecentra (WEC), de wet op het primair onderwijs (WPO), de wet op het voortgezet onderwijs (WVO) en de wet Medezeggenschap op scholen (WMS).

Voor de bescherming van de privacy van medewerkers van Visio zijn de wet verbetering poortwachter (WVP), de Arbowet en de Wet op de ondernemingsraden (WOR) van belang.

De AVG stelt het opstellen van privacybeleid (gegevensbeschermingsbeleid) verplicht als onderdeel van de verantwoordingsplicht. Dit als dat in verhouding staat tot de verwerkingsactiviteiten die Koninklijke Visio verricht. Gezien het feit dat Koninklijke Visio op grote schaal gezondheidsgegevens verwerkt, geldt dit zeker voor ons.

Op verzoek van een betrokkene (cliënt, leerling, medewerker) stellen wij ons privacybeleid en privacyreglement ter beschikking.

## Voor wie is dit reglement bedoeld?

Dit privacyreglement is bedoeld voor alle medewerkers, waaronder inhuurkrachten, vrijwilligers en stagiaires van Koninklijke Visio. Zij zijn bij de start van hun werkzaamheden bij Koninklijke Visio op dit privacyreglement gewezen. Iedere medewerker is gehouden om aan de vereisten in dit privacyreglement te voldoen. Dit reglement, in combinatie met het privacybeleid, kan tevens worden gebruikt voor het informeren van leerlingen, cliënten en vertegenwoordigers over hoe Koninklijke Visio omgaat met Persoonsgegevensbescherming.

Voor vragen over het privacyreglement en het beleid voor de bescherming van persoonsgegevens kunnen medewerkers terecht bij de manager / schoolleider of op [privacy@visio.org](mailto:privacy@visio.org). De functionaris gegevensbescherming is te bereiken via [privacy@visio.org](mailto:privacy@visio.org) of op telefoonnummer 088-585 5777. Het privacyreglement wordt gepubliceerd op intranet, waar ook meer informatie over de bescherming van persoonsgegevens is te vinden, en tevens op de website van Visio.

# Uitgangspunten verwerking Persoonsgegevens

## Verwerking van Persoonsgegevens

Onder Persoonsgegevens verstaan we alle informatie die over een persoon gaat, of herleidbaar is tot een persoon. Bijvoorbeeld een naam, telefoonnummer of emailadres. Maar ook IP-adressen zijn Persoonsgegevens. Bijzondere Persoonsgegevens, zoals gezondheidsgegevens krijgen extra bescherming volgens de privacywet. De privacywetgeving is van toepassing als we te maken hebben met een verwerking van Persoonsgegevens. Hier is al snel sprake van. Verwerking is het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of in een andere vorm beschikbaar stellen, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens.

## Beginselen inzake persoonsgegevens verwerking

Koninklijke Visio is verantwoordelijk voor de naleving van onderstaande beginselen bij de verwerking van persoonsgegevens en moet de naleving van deze beginselen kunnen aantonen (“verantwoordingsplicht”). Binnen Koninklijke Visio worden persoonsgegevens alleen verwerkt:

1. op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is;
2. voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden en mogen vervolgens niet verder op een met die doeleinden onverenigbare wijze worden verwerkt; de verdere verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden wordt niet als onverenigbaar met de oorspronkelijke doeleinden beschouwd (“doelbinding”);[[1]](#footnote-1)
3. voor zover zij toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt (“minimale gegevensverwerking” ook wel “dataminimalisatie”);
4. indien de persoonsgegevens juist zijn en zo nodig worden geactualiseerd. Alle redelijke maatregelen moeten worden genomen om de persoonsgegevens die, gelet op de doeleinden waarvoor zij worden verwerkt, onjuist zijn, onverwijld te wissen of te rectificeren (“juistheid”)
5. en bewaard in een vorm die het mogelijk maakt de betrokkenen niet langer te identificeren dan voor de doeleinden waarvoor de persoonsgegevens worden verwerkt noodzakelijk is; persoonsgegevens mogen voor langere perioden worden opgeslagen voor zover de persoonsgegevens louter met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden worden verwerkt mits de bij deze verordening vereiste passende technische en organisatorische maatregelen worden getroffen om de rechten en vrijheden van de betrokkene te beschermen (“opslagbeperking”);
6. door het nemen van passende technische of organisatorische maatregelen op een dusdanige manier dat een passende beveiliging ervan gewaarborgd is, en dat zij onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging (“integriteit en vertrouwelijkheid”).

## 2.3 Doeleinden bij verwerking van persoonsgegevens domein onderwijs

Voor het domein onderwijs van Visio zijn de doeleinden van toepassing zoals vastgelegd door de PO raad in het Convenant digitale onderwijsmiddelen en privacy. Deze zijn opgenomen in bijlage 2.

# Rechtmatige gegevensverwerking

## Voorwaarden verwerking Persoonsgegevens

Persoonsgegevens mogen alléén worden verwerkt als aan een van de onderstaande voorwaarden is voldaan:

* de betrokkene heeft toestemminggegeven voor de verwerking van zijn Persoonsgegevens voor één of meer specifieke doeleinden.

*Koninklijke Visio moet kunnen aantonen dat toestemming is gegeven. Toestemming wordt daarom zoveel mogelijk schriftelijk gevraagd en vastgelegd in het elektronisch dossier van de cliënt, leerling of medewerker. Ook moet de toestemming voldoende specifiek en geïnformeerd zijn en vrijelijk zijn gegeven. Toestemming wordt zoveel mogelijk op voorhand, bij inschrijving van de leerling, start behandeling cliënt of indiensttreding medewerker vastgelegd.*

*Betrokkenen hebben altijd het recht hun toestemming weer in te trekken. Bij indiening van het verzoek wordt de verwerking waarvoor toestemming is gegeven, direct gestopt. Het intrekken van toestemming doet geen afbreuk aan de rechtmatigheid van de verwerking op basis van de toestemming vóór de intrekking daarvan.*

* de gegevensverwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, bijvoorbeeld de behandelingsovereenkomst of de arbeidsovereenkomst;
* de gegevensverwerking is noodzakelijk om een wettelijke verplichting na te komen, bijvoorbeeld de dossierplicht in de Wgbo of gegevensverstrekking bij gedwongen opname en gedwongen behandeling op grond van de Wet zorg en dwang;
* de gegevensverwerking is noodzakelijk ter bescherming van de vitale belangen van de betrokkene of een ander natuurlijk persoon;
* de gegevensverwerking is noodzakelijk voor de goede vervulling van een taak van algemeen belang, dat elders in een wet is vastgelegd met eventuele nadere bepalingen;
* de gegevensverwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde én de belangen, grondrechten of fundamentele vrijheden van degene van wie de gegevens worden verwerkt niet prevaleren.

## Voorwaarden voor het verwerken van gezondheidsgegevens

Gezondheidsgegevens zijn één van de categorieën bijzondere Persoonsgegevens. Het is in de AVG verboden bijzondere categorieën Persoonsgegevens te verwerken, tenzij voldaan wordt aan één van de wettelijke voorwaarden uit artikel 9 AVG. Voor Koninklijke Visio zijn onderstaande voorwaarden van toepassing:

* Als de verwerking noodzakelijk is voor doeleinden van preventieve of arbeidsgeneeskunde, voor de beoordeling van de arbeidsgeschiktheid van de werknemer, medische diagnosen, het verstrekken van gezondheidszorg of sociale diensten of behandelingen dan wel het beheren van gezondheidszorgstelsels en -diensten of sociale stelsels en diensten, voor zover dit is toegestaan in nationale wetgeving.

Zo mogen gegevens over gezondheid worden verwerkt met het doel gezondheidszorg te leveren, onder de verantwoordelijkheid van een beroepsbeoefenaar die aan het beroepsgeheim gebonden is of door een ander persoon die op grond van de wet of overeenkomst tot geheimhouding is gehouden.

* De verwerking is noodzakelijk om redenen van zwaarwegend algemeen belang, op grond van Unierecht of lidstatelijk recht, waarbij de evenredigheid met het nagestreefde doel wordt gewaarborgd, de wezenlijke inhoud van het recht op bescherming van persoonsgegevens wordt geëerbiedigd en passende en specifieke maatregelen worden getroffen ter bescherming van de grondrechten en de fundamentele belangen van de betrokkene.

In het kader hiervan is het Domein Onderwijs in bepaalde gevallen toegestaan gezondheidsgegevens van leerlingen te verwerken. Dit is opgenomen in artikel 30 lid 2 UAVG.

Nb.: naast de opheffing van het verbod om bijzondere gezondheidsgegevens te verwerken zoals hierboven genoemd, moet ook nog een verwerkingsgrondslag (zie hoofdstuk 3.1) aanwezig zijn om dergelijke gegevens te verwerken.

## Wanneer mogen andere bijzondere gegevens dan de gezondheidsgegevens worden verwerkt?

Andere bijzondere gegevens, bijvoorbeeld gegevens met betrekking tot ras/etniciteit of godsdienst/ levensovertuiging mogen alleen als aanvulling op gezondheidsgegevens worden verwerkt als dat nodig is voor een goede behandeling of verzorging van de betrokkene en dus niet systematisch bij elke cliënt. Bijvoorbeeld voor de inschakeling van een beëdigd tolk/vertaler als dat voor de uitleg van de behandeling aan cliënt nodig is.

## Gegevensverwerking door een verwerker

Koninklijke Visio kan de verwerking (extern) uitbesteden aan een verwerker. Bijvoorbeeld voor salarisverwerking of bij hosting van persoonsgegevens. In een verwerkersovereenkomst worden de verplichtingen uit de AVG opgelegd aan de verwerker.

Koninklijke Visio doet uitsluitend een beroep op verwerkers die afdoende garanties met betrekking tot het toepassen van passende technische en organisatorische maatregelen bieden opdat de verwerking aan de vereisten van deze verordening voldoet en de bescherming van de rechten van de betrokkene is gewaarborgd. Koninklijke Visio controleert dit voordat de overeenkomst wordt afgesloten.

De verwerking door een verwerker wordt geregeld in een (verwerkers)overeenkomst die de verwerker ten aanzien van Koninklijke Visio bindt en waarin het onderwerp, de duur van de verwerking, de aard en het doel van de verwerking, het soort persoonsgegevens en de categorieën van betrokkenen en de rechten en verplichtingen van Koninklijke Visio worden omschreven. Een dergelijke overeenkomst dient te voldoen aan de eisen die de AVG daaraan stelt.

Koninklijke Visio maakt in principe gebruik van een modelovereenkomst die is gebaseerd op de zogenaamde BOZ-modelverwerkersovereenkomst. De inhoud van alle af te sluiten verwerkersovereenkomsten wordt beoordeeld door de functionaris voor gegevensbescherming.

Wanneer het gaat om afspraken met leveranciers over digitale onderwijsmiddelen waarbij persoonsgegevens worden verwerkt, wordt gebruik gemaakt van het Model Verwerkersovereenkomst Digitale onderwijsmiddelen en privacy versie 3.0 – maart 2018.

De verwerker en eenieder die onder het gezag van Koninklijke Visio of van de verwerker handelt en toegang heeft tot persoonsgegevens, verwerkt deze uitsluitend in opdracht van Koninklijke Visio, tenzij hij door wet- of regelgeving tot verwerking gehouden is.

## Gezamenlijke verwerkingsverantwoordelijken

Wanneer twee of meer verwerkingsverantwoordelijken gezamenlijk de doeleinden en middelen van de verwerking bepalen, zijn zij gezamenlijk verwerkingsverantwoordelijken. Zij stellen op transparante wijze hun respectieve verantwoordelijkheden voor de nakoming van de verplichtingen uit hoofde van deze AVG vast, met name met betrekking tot de uitoefening van de rechten van de betrokkene en hun respectieve verplichtingen om de verplichte informatie te verstrekken, door middel van een onderlinge regeling. In de regeling kan een contactpunt voor betrokkenen worden aangewezen. Uit de bedoelde regeling blijkt duidelijk welke rol de gezamenlijke verwerkingsverantwoordelijken respectievelijk vervullen, en wat hun respectieve verhouding met de betrokkenen is. De wezenlijke inhoud van de regeling wordt aan de betrokkene beschikbaar gesteld. Ongeacht een dergelijke regeling kan een betrokkene zijn rechten uit de AVG met betrekking tot en jegens iedere verwerkingsverantwoordelijke uitoefenen.

## Aansprakelijkheid verwerkingsverantwoordelijke en/of verwerker

Koninklijke Visio is als verwerkingsverantwoordelijke verantwoordelijk en aansprakelijk voor schade die voortvloeit uit het toerekenbaar tekortschieten of niet voldoende naleven van de AVG, waaronder het wel/niet naleven van de beveiligingseisen.

De verwerker, waaraan Koninklijke Visio (een deel van) gegevensverwerking heeft uitbesteed, kan daarnaast zelfstandig aansprakelijk zijn voor schade of een deel van de schade die voortvloeit uit zijn werkzaamheden. Hoe die aansprakelijkheid wordt verdeeld, wordt beoordeeld door de schadeverzekeraar of de rechter. Van belang is dat Koninklijke Visio goede afspraken maakt met de verwerker en deze vastlegt in een verwerkersovereenkomst.

# Verstrekking van gegevens aan derden

## Geheimhoudingsplicht

Voor alle medewerkers van Koninklijke Visio geldt een geheimhoudingsplicht. Dit is geregeld in een overeenkomst bij de aanstelling. Daarnaast geldt voor Persoonsgegevens verkregen in de uitoefening van een beroep in de (geestelijke) gezondheidszorg de geheimhoudingsplicht van de hulpverlener. Deze geheimhoudingsplicht is o.a. vastgelegd in de Wgbo en/of Jeugdwet en de wet BIG en in verschillende beroepscodes. Vanwege de geheimhoudingsplicht mogen medewerkers géén gegevens verstrekken aan personen of instanties binnen en buiten Koninklijke Visio, tenzij aan een aantal voorwaarden is voldaan. Let wel: ondanks dat aan deze voorwaarden is voldaan, houdt Koninklijke Visio haar verantwoordelijkheid om proportioneel te handelen. Dat houdt in dat gegevens alleen worden gedeeld die echt noodzakelijk zijn om te verstrekken.

## Verstrekking van cliëntgegevens aan derden

### Informatie uitwisseling met rechtstreeks betrokkenen

Zorgverleners mogen medische informatie delen met anderen die rechtstreeks betrokken zijn bij de uitvoering van de behandelingsovereenkomst en met degene die optreedt als vervanger van de hulpverlener. Dit mag alleen als die informatie noodzakelijk is voor hun werkzaamheden.

### Toestemming

Je mag informatie aan derden verstrekken als cliënten, leerlingen of medewerkers hiervoor toestemming hebben gegeven, tenzij een andere rechtsgrond, zoals bedoeld in hoofdstuk 3 van toepassing is. Uit de gegeven toestemming moet blijken dat deze vrijelijk, specifiek en geïnformeerd is gegeven. Toestemming wordt altijd vastgelegd in het elektronisch dossier van de betrokkene, onder vermelding van datum van toestemming.

Intrekken van toestemming

Betrokkenen hebben altijd het recht hun toestemming weer in te trekken. Verzoeken om intrekken van toestemming worden ingediend bij de locatiemanager, schoolleiding of HRadministratie. Bij indiening van het verzoek wordt de verwerking waarvoor toestemming is gegeven, direct gestopt. Het intrekken van toestemming doet geen afbreuk aan de rechtmatigheid van de verwerking op basis van de toestemming vóór de intrekking daarvan.

Verwijzing medisch specialist

Bij een verwijzing naar een medisch specialist is het gebruikelijk dat medische informatie over de cliënt wordt meegestuurd. Omdat de cliënt instemt met de verwijzing, wordt verondersteld dat de laatstgenoemde ook voor het verstrekken van informatie aan de medisch specialist toestemming geeft. Hiervoor hoeft dus niet opnieuw toestemming worden gevraagd.

Toestemming bij terugkoppeling naar verwijzer

Voor terugkoppelingen van specialisten naar verwijzers is toestemming nodig van de cliënt.

Opvragen cliëntgegevens bij derden

Als het voor de zorg- en ondersteuning nodig is om cliëntgegevens bij externe partijen op te vragen, dan dient de medewerker hiervoor de toestemming van de cliënt te vragen.

Opvragen leerlinggegevens bij derden

Voor het opvragen van leerlinggegevens bij derden is, als geen andere rechtsgrond (hoofdstuk 3) van toepassing is, toestemming van de leerling/ouder noodzakelijk.

### Wettelijke verplichting

Gegevens moeten worden verstrekt als hiervoor een wettelijke verplichting is. Dit is bijvoorbeeld het geval voor verstrekkingen aan gemeenten en/of zorgkantoren in het kader van de Wmo, wlz, jeugdwet en de leerplichtwet of de verstrekking van bepaalde gegevens van medewerkers aan de belastingdienst. Let wel: verstrekkingen in het kader van een wettelijke verplichting betekent niet dat alle gegevens verstrekt mogen worden. De verstrekking bevat altijd specifieke gegevens voor specifieke doeleinden. Ook dient de betrokkene op de hoogte gesteld te worden van deze verstrekkingen.

### Conflict van plichten

Als geen toestemming verkregen kan worden, maar de zorgprofessional ernstige schade aan de cliënt of aan een ander kan voorkomen door informatie aan een derde te verstrekken, dan mag informatie met een beroep op een conflict van plichten aan derden worden verstrekt. Daarbij moet wel aan de volgende voorwaarden zijn voldaan:

* Alles is in het werk gesteld om eerst toestemming van de cliënt te verkrijgen.
* De zwijgplichtige zorgprofessional verkeert in gewetensnood door het handhaven van de zwijgplicht.
* Er is geen andere weg dan doorbreking van het geheim om het probleem op te lossen.
* Het niet doorbreken van de zwijgplicht levert voor een ander ernstige schade op.
* Het moet vrijwel zeker zijn dat de door de geheimdoorbreking schade kan worden voorkomen of beperkt.

Wanneer de geheimhoudingsplicht (en het beroepsgeheim) op basis van ‘conflict van plichten’ wordt doorbroken, dan moet het geheim zo min mogelijk geschonden worden. Alleen direct relevante gegevens mogen verstrekt worden. Voor zover mogelijk moet je ook aan een cliënt melden dat gegevens aan een ander zijn verstrekt.

### Meldrechten

In bepaalde gevallen geldt er een meldrecht. Bijvoorbeeld bij vermoedens van kindermishandeling en huiselijk geweld.

# Gebruik van gegevens voor wetenschappelijk onderzoek

## Wanneer mogen gegevens aan een ander worden verstrekt voor wetenschappelijk onderzoek en statistiek op het gebied van de volksgezondheid?

De gegevensverwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden is onderworpen aan passende waarborgen in overeenstemming met de AVG voor de rechten en vrijheden van de betrokkene. De waarborgen zorgen ervoor dat er technische en organisatorische maatregelen zijn getroffen om de inachtneming van het beginsel van minimale gegevensverwerking te garanderen. Deze maatregelen kunnen pseudonimisering omvatten, mits aldus die doeleinden in kwestie kunnen worden verwezenlijkt. Wanneer die doeleinden kunnen worden verwezenlijkt door verdere verwerking die de identificatie van betrokkenen niet of niet langer toelaat, moeten zij aldus worden verwezenlijkt. Tevens kan er in nationale wetgeving worden afgeweken van bepaalde rechten van betrokkenen uit de AVG voor zover die rechten de verwezenlijking van de specifieke doeleinden onmogelijk dreigen te maken of ernstig dreigen te belemmeren, en dergelijke afwijkingen noodzakelijk zijn om die doeleinden te bereiken.

De Wgbogeeft onderstaande afwijkende bepalingen voor wetenschappelijk onderzoek op het gebied de van gezondheidszorg. Het uitgangspunt is dat voor het verstrekken van niet geanonimiseerde gegevens toestemming van de cliënt is vereist. In afwijking van dit uitgangspunt kan ook zonder toestemming van de cliënt ten behoeve van statistiek of wetenschappelijk onderzoek op het gebied van de volksgezondheid aan een ander desgevraagd inlichtingen over de cliënt of inzage in de bescheiden, worden verstrekt indien:

* het vragen van toestemming in redelijkheid niet mogelijk is en bij de uitvoering van het onderzoek zodanige waarborgen gelden, dat de persoonlijke levenssfeer van de cliënt niet onevenredig wordt geschaad, of
* het vragen van toestemming, gelet op de aard en het doel van het onderzoek, in redelijkheid niet kan worden verlangd en de hulpverlener ervoor zorgt dat gegevens in zodanige vorm worden verstrekt dat herleiding tot individuele natuurlijke personen redelijkerwijs wordt voorkomen.

Verder moet:

* het onderzoek een algemeen belang dienen;
* aangetoond zijn dat het onderzoek niet zonder de gegevens kan worden uitgevoerd; en
* de betrokken cliënt tegen een verstrekking niet uitdrukkelijk bezwaar hebben gemaakt.

Belangrijk om te beseffen is dat bovenstaande voorwaarden cumulatief werken; verstrekking is pas mogelijk indien aan alle voorwaarden is voldaan.

## Afspraken met de onderzoeker

Koninklijke Visio en de onderzoeker maken schriftelijke afspraken over de maatregelen die de onderzoeker neemt om de privacy van betrokkenen te beschermen. Deze afspraken staan in de samenwerkingsovereenkomst. In de samenwerkingsovereenkomst is opgenomen dat de onderzoeker toestemming vraagt aan de cliënt, waarbij gebruik wordt gemaakt van het toestemmingsformulier van Koninklijke Visio. Toestemmingsformulieren worden opgeslagen in het elektronisch dossier van de cliënt.

# Rechten van betrokkenen

## Voorwaarden met betrekking tot de uitvoering van de rechten van de betrokkenen

Het verstrekken van de in dit hoofdstuk bedoelde informatie, het verstrekken van de communicatie en het treffen van de maatregelen geschieden kosteloos. Indien het verzoek kennelijk ongegrond of buitensporig is, met name vanwege het repetitieve karakter, mag Koninklijke Visio:

* een redelijke vergoeding aanrekenen in het licht van de administratieve kosten waarmee het verstrekken van de gevraagde informatie of communicatie en het treffen van de gevraagde maatregelen gepaard gaan; ofwel
* weigeren gevolg te geven aan het verzoek.

Het is aan Koninklijke Visio om de kennelijk ongegronde of buitensporige aard van het verzoek aan te tonen.

Koninklijke Visio verstrekt de betrokkene onverwijld en in ieder geval binnen een maand na ontvangst van het verzoek krachtens dit hoofdstuk informatie over het gevolg dat aan het verzoek is gegeven. Afhankelijk van de complexiteit van het verzoek en van het aantal verzoeken kan die termijn indien nodig met nog eens twee maanden worden verlengd. Koninklijke Visio stelt de betrokkene binnen één maand, na ontvangst van het verzoek, in kennis van een dergelijke verlenging. Wanneer de betrokkene zijn verzoek elektronisch indient, wordt de informatie indien mogelijk elektronisch verstrekt, tenzij de betrokkene anderszins verzoekt.

Als Koninklijke Visio het verzoek van betrokkene afwijst, geeft hij daarvan schriftelijk de reden. Koninklijke Visio deelt een afwijzing van het verzoek onverwijld en uiterlijk binnen één maand na ontvangst van het verzoek aan de verzoeker mee. Ook informeert Koninklijke Visio de verzoeker over de mogelijkheid om een klacht in te dienen bij de Autoriteit Persoonsgegevens en de mogelijkheid om beroep in te stellen bij de rechter.

Betrokkenen kunnen verzoeken voor de uitoefening van hun rechten richten tot de locatiemanager, schoolleiding of HRadministratie. Om verzoeken van betrokkenen in te willigen wordt de identiteit van de betrokkene gecontroleerd. Dit is noodzakelijk om te verifiëren dat verzoeken niet onrechtmatig (door onbevoegden) worden ingediend.

## Recht op inzage en afschrift/kopie

Inzagerecht cliënten[[2]](#footnote-2)

De betrokken cliënt van twaalf jaar of ouder heeft recht op inzage en een kopie van de op zijn of haar persoon betrekking hebbende verwerkte gegevens. De inzage of afschrift verstrekking vindt plaats voor zover daarbij de persoonlijke levenssfeer van een ander niet wordt geschaad. Bijvoorbeeld: informatie over, of verstrekt door derden (niet-professionals), zoals familie en naastbetrokkenen of omstanders, wordt niet zonder voorafgaande toestemming van die derde verstrekt.

Een wettelijk vertegenwoordiger van jongeren onder de 16 jaar of van een wilsonbekwame volwassene, heeft recht op inzage in, of afschrift van het dossier met dezelfde uitzondering voor informatie over of verstrekt door derden (de andere ouder, familie, naastbetrokkenen en omstanders) voor zover van die vertegenwoordigers toestemming voor de behandeling is vereist.[[3]](#footnote-3) De vertegenwoordiger krijgt alleen die informatie die noodzakelijk is voor het uitoefenen van zijn taken als vertegenwoordiger.

Indien de hulpverlener door inlichtingen over de cliënt dan wel inzage in of afschrift van de bescheiden aan de (wettelijk) vertegenwoordiger te verstrekken niet geacht kan worden de zorg van een goed hulpverlener in acht te nemen, laat hij zulks achterwege.[[4]](#footnote-4) Bijvoorbeeld als een minderjarige bezwaar maakt tegen het verstrekken van (bepaalde) informatie aan de ouders of bij een vermoeden van kindermishandeling. In dat geval kan een ouder inzage in het dossier van de minderjarige worden geweigerd. Onder omstandigheden kan de hulpverlener in dat geval feitelijk worden belemmerd om de wettelijk vertegenwoordigers voldoende te informeren om hun toestemming voor de behandeling van de minderjarige te verkrijgen.

Cliënten kunnen inzage krijgen in hun dossier via het cliëntenportaal. Inzageverzoeken voor gegevens die niet via het cliëntenportaal beschikbaar zijn kunnen worden gericht aan de locatiemanager.

Inzagerecht leerlingen

Leerlingen die ouder zijn dan 16 jaar, dan wel de ouders van leerlingen jonger dan 16 jaar, kunnen zich met inzageverzoeken wenden tot het digitale inzageportaal. Inzageverzoeken die niet via het inzageportaal beschikbaar zijn, worden gericht aan de schoolleiding.

Visio kan privacy verzoeken als bedoeld in dit hoofdstuk weigeren, ter bescherming van de leerling of ter bescherming van de rechten en vrijheden van anderen.[[5]](#footnote-5) De weigering wordt schriftelijk en voldoende gemotiveerd vastgelegd.

Inzagerecht medewerkers

Medewerkers kunnen inzage krijgen in hun personeelsdossier via Afas Insite. Inzageverzoeken voor gegevens die niet via Afas Insite beschikbaar zijn kunnen worden gericht aan de HR administratie.

## Recht op informatie

### Te verstrekken informatie

Als Koninklijke Visio gegevens bij de betrokkene zelf opvraagt om te verwerken, informeert hij de betrokkene in een beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke vorm, voorafgaand aan het verkrijgen van zijn persoonsgegevens, over:

* de identiteit en de contactgegevens van Koninklijke Visio;
* de contactgegevens van de Functionaris voor Gegevensbescherming
* de verwerkingsdoelen waarvoor de gegevens zijn bestemd, en de rechtsgrond voor de verwerking;
* in voorkomend geval, de ontvangers of categorieën van ontvangers van de Persoonsgegevens.

Daarnaast dient onderstaande aanvullende informatie te worden verstrekt om behoorlijke en transparante verwerking te waarborgen:

* de periode gedurende welke de persoonsgegevens zullen worden opgeslagen of indien dat niet mogelijk is, de criteria ter bepaling van die termijn;
* de mogelijkheden die de betrokkene heeft om een verzoek om inzage, rectificatie of wissing van de persoonsgegevens of beperking van de hem betreffende verwerking, alsmede het recht tegen de verwerking bezwaar te maken en het recht op gegevensoverdraagbaarheid;
* Indien de gegevensverwerking op toestemming is gebaseerd, dient de betrokkene geïnformeerd te worden over het recht om te allen tijde die toestemming in te trekken, zonder dat dit afbreuk doet aan de rechtmatigheid van de verwerking op basis van de toestemming voor de intrekking daarvan.
* het recht een klacht in te dienen bij de Autoriteit Persoonsgegevens en op welke wijze de betrokkene deze rechten kan inroepen.
* of de verstrekking van persoonsgegevens een wettelijke of contractuele verplichting is dan wel een noodzakelijke voorwaarde om een overeenkomst te sluiten en of de betrokkene verplicht is de persoonsgegevens te verstrekken en wat de mogelijke gevolgen zijn wanneer deze gegevens niet worden verstrekt.

Wanneer Koninklijke Visio voornemens heeft de persoonsgegevens verder te verwerken voor een ander doel dan waarvoor de persoonsgegevens zijn verzameld, verstrekt Koninklijke Visio de betrokkene vóór die verdere verwerking informatie over dat andere doel en alle relevante verdere informatie als bedoeld in het tweede lid van deze bepaling.

Bovenstaande is niet van toepassing wanneer en voor zover de betrokkene reeds over de informatie beschikt.

### Te verstrekken informatie wanneer de persoonsgegevens niet van de betrokkene zijn verkregen

Wanneer persoonsgegevens niet van de betrokkene zijn verkregen, verstrekt Koninklijke Visio de betrokkene alle informatie conform hierboven en bovendien de betrokken categorieën van persoonsgegevens alsmede de bron waar de persoonsgegevens vandaan komen.

Koninklijke Visio verstrekt de in hoofdstuk 6.3.1 bedoelde informatie:

* binnen een redelijke termijn, maar uiterlijk binnen één maand na de verkrijging van de persoonsgegevens, afhankelijk van de concrete omstandigheden waarin de persoonsgegevens worden verwerkt;
* indien de persoonsgegevens zullen worden gebruikt voor communicatie met de betrokkene, uiterlijk op het moment van het eerste contact met de betrokkene; of
* indien verstrekking van de gegevens aan een andere ontvanger wordt overwogen, uiterlijk op het tijdstip waarop de persoonsgegevens voor het eerst worden verstrekt.
* Wanneer Koninklijke Visio voornemens heeft om de persoonsgegevens verder te verwerken voor een ander doel dan dat waarvoor de persoonsgegevens zijn verkregen, verstrekt Koninklijke Visio de betrokkene vóór die verdere verwerking informatie over dat andere doel en alle relevante verdere informatie als bedoeld in het eerste lid van dit artikel.

Koninklijke Visio hoeft de betrokkene niet te informeren over de hiervoor genoemde informatie indien:

* de betrokkene al over de informatie beschikt;
* het informeren van betrokkene onmogelijk blijkt of een onevenredige inspanning kost. In het bijzonder bij verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden, behoudens de in artikel 89, lid 1, AVG bedoelde voorwaarden en waarborgen, of voor zover de in dit artikel bedoelde verplichting de verwezenlijking van de doeleinden van die verwerking onmogelijk dreigt te maken of ernstig in het gedrang dreigt te brengen. In dergelijke gevallen neemt Koninklijke Visio passende maatregelen om de rechten, de vrijheden en de gerechtvaardigde belangen van de betrokkene te beschermen, waaronder het openbaar maken van de informatie;
* het verkrijgen of verstrekken van informatie (zoals hiervoor genoemd) op grond van wet- en regelgeving verplicht is voor Koninklijke Visio en die wet- en regelgeving voorziet in passende maatregelen om de gerechtvaardigde belangen van de betrokkene te beschermen; of
* de persoonsgegevens vertrouwelijk moeten blijven uit hoofde van een beroepsgeheim in het kader van wet- en regelgeving, waaronder een statutaire geheimhoudingsplicht.

### Wijze van informatieverstrekking

De informatie wordt door middel van een privacy statement aangeboden. Voor cliënten, leerlingen, medewerkers, sollicitanten en op de website zijn verschillende privacy statements beschikbaar. Koninklijke Visio stelt deze privacy statements actief beschikbaar bij het eerste contactmoment met cliënten, leerlingen en medewerkers (waaronder externen, stagiaires en vrijwilligers). Dit is in ieder geval op het moment van aanmelding van de cliënt of op het eerste contactmoment van de cliënt met Koninklijke Visio, op het moment van indiensttreding van medewerkers (waaronder stagiaires, vrijwilligers en externen), op het moment dat leerlingen zich inschrijven en bij het eerste contact met de sollicitant. Wanneer betrokkenen vragen hebben over hun Persoonsgegevensbescherming, wordt door Koninklijke Visio naar dit privacy statement verwezen.

## Recht op gegevensoverdraagbaarheid (dataportabiliteit)

De betrokkene heeft het recht de hem betreffende Persoonsgegevens, die hij aan Koninklijke Visio heeft verstrekt, in een gestructureerde, gangbare en machineleesbare vorm te verkrijgen en heeft het recht die gegevens aan een andere verwerkingsverantwoordelijke (bijvoorbeeld andere zorgaanbieder) over te dragen, zonder daarbij te worden gehinderd door Koninklijke Visio, indien de verwerking berust op toestemming of op uitvoering van een overeenkomst en de verwerking geautomatiseerd wordt verricht. Bij de uitoefening van het recht op gegevensoverdraagbaarheid heeft de betrokkene het recht dat de Persoonsgegevens, indien dit technisch mogelijk is, rechtstreeks van de ene zorg- of onderwijsaanbieder naar de andere worden doorgezonden. Bij de uitoefening van dit recht mag dit geen afbreuk doen aan de rechten en vrijheden van anderen.

## Recht op rectificatie, aanvulling en beperking van Persoonsgegevens

De betrokkene kan Koninklijke Visio vragen om rectificatie (verbetering) van de hem of haar betreffende Persoonsgegevens als die onjuist zijn of Koninklijke Visio verzoeken om vervollediging van zijn of haar Persoonsgegevens. Dit met in achtneming van het doel van de verwerking, onder meer door een eigen aanvullende verklaring toe te voegen aan zijn dossier. Betrokkenen kunnen ook aan Koninklijke Visio vragen om bepaalde gegevens voor bepaalde personen af te schermen en hen de toegang tot die gegevens te laten blokkeren

Cliënten, leerlingen en medewerkers kunnen hiervoor respectievelijk terecht bij de locatiemanager, schoolleiding en HRaministratie. Het verzoek van een betrokkene en beslissing van Koninklijke Visio tot rectificatie (verbetering), aanvulling of beperking van gegevens blijft bewaard in het dossier van de cliënt, leerling of medewerker.

## Recht op gegevenswissing (recht op vergetelheid)

De betrokkene heeft het recht van Koninklijke Visio zonder onredelijke vertraging wissing van hem betreffende Persoonsgegevens te verkrijgen. Koninklijke Visio is verplicht deze Persoonsgegevens te wissen wanneer een van de volgende gevallen van toepassing is:

* de Persoonsgegevens zijn niet langer nodig voor de doeleinden waarvoor zij zijn verzameld of anderszins zijn verwerkt;
* de betrokkene trekt de toestemming waarop de verwerking berust in en er is geen andere rechtsgrond voor de verwerking;
* de Persoonsgegevens zijn onrechtmatig verwerkt;
* de Persoonsgegevens moeten worden gewist op basis van een wettelijke verplichting die op Koninklijke Visio rust.

Koninklijke Visio stelt iedere ontvanger aan wie Persoonsgegevens zijn verstrekt, in kennis van de wissing (verwijdering) van Persoonsgegevens tenzij dit onmogelijk blijkt of onevenredig veel inspanning vergt. Koninklijke Visio verstrekt de betrokkene informatie over deze ontvangers indien de betrokkene hierom verzoekt.

Wanneer Koninklijke Visio de Persoonsgegevens openbaar heeft gemaakt en verplicht is de Persoonsgegevens te wissen, neemt zij, rekening houdend met de beschikbare technologie en de uitvoeringskosten, redelijke maatregelen, waaronder technische maatregelen, om verwerkingsverantwoordelijken die de Persoonsgegevens verwerken, ervan op de hoogte te stellen dat de betrokkene de verwerkingsverantwoordelijken heeft verzocht om iedere koppeling naar, of kopie of reproductie van die Persoonsgegevens te wissen.

Indien het gezondheidsgegevens betreft, wist Koninklijke Visio de gegevens zonder onredelijke vertraging en verstrekt de betrokkene in ieder geval binnen een maand na ontvangst van het verzoek informatie over het gevolg dat aan het verzoek is gegeven. Afhankelijk van de complexiteit van de verzoeken en van het aantal verzoeken kan die termijn indien nodig met nog eens twee maanden worden verlengd. Koninklijke Visio stelt de betrokkene binnen één maand na ontvangst van het verzoek in kennis van een dergelijke verlenging.

Een verzoek tot gegevenswissing mag alleen worden geweigerd als:

* de wet zich tegen de vernietiging verzet;   
  Bijvoorbeeld: het dossier aangelegd binnen een gedwongen behandeling moet vijf jaar na beëindiging van de WZD-behandeling of verblijf in het ziekenhuis bewaard blijven. Een verzoek van een cliënt tot vernietiging binnen vijf jaar kan niet worden gehonoreerd;
* een derde een aanmerkelijk belang heeft bij bewaring van die gegevens. Bijvoorbeeld: een kind van een cliënt heeft een erfelijke ziekte;
* de cliënt heeft een procedure tegen de hulpverlener aangespannen of het is waarschijnlijk dat hij dit zal doen;
* in het dossier gegevens over (vermoedens van) kindermishandeling staan dan kunnen deze gegevens op grond van de Meldcode Huiselijk Geweld en Kindermishandeling alleen op verzoek van het kind zelf worden vernietigd en uitsluitend als het kind de leeftijd van 16 jaar heeft bereikt en wilsbekwaam ter zake kan worden geacht;
* Koninklijke Visio de gegevens nodig heeft voor de instelling, uitoefening of onderbouwing van een rechtsvordering;
* om redenen van algemeen belang op het gebied van volksgezondheid.

Cliënten, leerlingen en medewerkers kunnen zich voor verzoeken tot wissing van gegevens wenden tot respectievelijk de locatiemanager, schoolleiding of HR administratie. Het verzoek tot wissing van een betrokkene en reactie van Koninklijke Visio hierop blijft bewaard in het dossier van de cliënt, leerling of medewerker.

## Recht van bezwaar

De betrokkene heeft te allen tijde het recht om vanwege met zijn specifieke situatie verband houdende redenen, bezwaar te maken tegen de verwerking van hem betreffende persoonsgegevens. Dit op basis van de noodzakelijkheid voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan Koninklijke Visio is opgedragen of op basis van de noodzakelijkheid voor de behartiging van de gerechtvaardigde belangen van Koninklijke Visio of van een derde;

Koninklijke Visio beoordeelt onverwijld en in ieder geval binnen één maand na ontvangst van het bezwaar of het bezwaar gerechtvaardigd is. Indien het bezwaar gerechtvaardigd is, beëindigt hij onmiddellijk de verwerking, tenzij er sprake is van dwingende gerechtvaardigde gronden voor de verwerking die zwaarder wegen dan de belangen, vrijheden en rechten van de betrokkene of die verband houden met de instelling, uitoefening of onderbouwing van een rechtsvordering.

## Vertegenwoordiging van cliënten

### Jeugdige cliënt jonger dan 12 jaar of wilsonbekwame jeugdige van 12 tot 18 jaar

Bij een jeugdige cliënt jonger dan twaalf jaar en bij een wilsonbekwame jeugdige van twaalf tot achttien jaar, oefent (oefenen) de ouder(s) met gezag of de voogd de rechten van de jeugdige cliënt uit, tenzij dit niet verenigbaar is met de zorg van een goed hulpverlener.[[6]](#footnote-6)

De ouder die geen gezag heeft krijgt desgevraagd belangrijke, algemene en feitelijke informatie[[7]](#footnote-7) over de gezondheidstoestand van de jeugdige cliënt, tenzij:

* de hulpverlener de informatie ook niet aan de ouder met gezag heeft verstrekt/ verstrekt;
* niet in niet verenigbaar is met de zorg van een goed hulpverlener.

### Wilsbekwame cliënt van twaalf jaar of ouder

De wilsbekwame cliënt van twaalf jaar of ouder oefent zelfstandig zijn rechten over zijn persoons- en gezondheidsgegevens met betrekking tot de behandelingsovereenkomst uit. Vernietiging van gegevens over (vermoedens van) kindermishandeling vindt uitsluitend plaats met toestemming van een wilsbekwame jeugdige van zestien jaar en ouder.

### Wilsonbekwame cliënt van 18 jaar en ouder

Is de betrokkene ouder dan achttien jaar en wilsonbekwaam ter zake, dan treedt als vertegenwoordiger voor hem op:

* een (toegewezen) curator of mentor;
* indien er geen curator of mentor is, de persoon die de cliënt schriftelijk heeft gemachtigd;
* indien de persoonlijk gemachtigde ontbreekt of niet optreedt; de echtgenoot of levensgezel van de betrokkene;
* indien de echtgenoot of levensgezel ontbreekt of niet optreedt: een kind, broer of zus van de betrokkene.

In het uiterste geval treedt Koninklijke Visio als zorgaanbieder op als goed hulpverlener. Koninklijke Visio zorgt er dan voor dat zo snel mogelijk een wettelijk vertegenwoordiger voor de betrokkene optreedt. Zo nodig, als familie of naaste dat niet kan of wil, verzoekt Koninklijke Visio de rechter om een vertegenwoordiger te benoemen.

# Bewaartermijnen

Koninklijke Visio dient de papieren en elektronische persoonsgegevens op een veilige wijze te bewaren, die in overeenstemming is met de geldende wet- en regelgeving. Persoonsgegevens worden niet langer bewaard dan noodzakelijk is om de doelen te bereiken waarvoor de gegevens worden verwerkt, tenzij de gegevens worden geanonimiseerd of indien het noodzakelijk is voor de uitoefening van het recht op vrijheid van meningsuiting en van informatie, voor de nakoming van een wettelijke verplichting, voor de uitvoering van een taak in het algemeen belang of in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is verleend, om redenen van algemeen belang op het vlak van volksgezondheid, met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden of voor de vaststelling, uitoefening of onderbouwing van een rechtsvordering.[[8]](#footnote-8)

Koninklijke Visio stelt vast hoelang de vastgelegde/geregistreerde persoonsgegevens bewaard blijven in overeenstemming met de geldende wet- en regelgeving. Indien nog geen specifieke termijn kan worden genoemd dan worden de criteria vastgesteld voor het vaststellen van de bewaartermijn.

Voor gezondheidsgegevens die binnen de zorgrelatie worden verwerkt, leerling- en personeelsgegevens, gelden verschillende bewaartermijnen. De bewaartermijnen van Koninklijke Visio staan benoemd in het bewaartermijnenbeleid van Koninklijke Visio.

# Veilige omgang met gegevens

## Verantwoordelijkheid van de verwerkingsverantwoordelijke

Rekening houdend met de aard, de omvang, de context en het doel van de verwerking, alsook met de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen, treft Koninklijke Visio passende technische en organisatorische maatregelen om te waarborgen en te kunnen aantonen dat de verwerking in overeenstemming met de AVG wordt uitgevoerd. Die maatregelen worden geëvalueerd en indien nodig geactualiseerd.

## Gegevensbescherming door ontwerp en standaardinstellingen (Privacy by design en default)

Koninklijke Visio treft passende technische en organisatorische maatregelen die zijn opgesteld met als doel de gegevensbeschermingsbeginselen, zoals minimale gegevensverwerking, op een doeltreffende manier uit te voeren en de nodige waarborgen in de verwerking in te bouwen ter naleving van de voorschriften van deze verordening en ter bescherming van de rechten van de betrokkenen. Deze maatregelen worden zowel bij de bepaling van de verwerkingsmiddelen als bij de verwerking zelf getroffen. Koninklijke Visio houdt hierbij rekening met de stand van de techniek, de uitvoeringskosten, en de aard, de omvang, de context en het doel van de verwerking alsook met de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen welke aan de verwerking zijn verbonden.

Koninklijke Visio treft passende technische en organisatorische maatregelen om ervoor te zorgen dat in beginsel alleen persoonsgegevens worden verwerkt die noodzakelijk zijn voor elk specifiek doel van de verwerking. Die verplichting geldt voor de hoeveelheid verzamelde persoonsgegevens, de mate waarin zij worden verwerkt, de termijn waarvoor zij worden opgeslagen en de toegankelijkheid daarvan. Deze maatregelen zorgen met name ervoor dat persoonsgegevens in beginsel niet zonder menselijke tussenkomst voor een onbeperkt aantal natuurlijke personen toegankelijk worden gemaakt.

Een goedgekeurd certificeringsmechanisme kan worden gebruikt als element om aan te tonen dat aan de voorschriften is voldaan.

Praktische uitwerking:

* Koninklijke Visio past de voor de veilige verwerking van zorggegevens de normen van de [NEN 7510, 7512 en 7513](https://www.nen.nl/Nieuws/Nieuws/NEN-7510-NEN-7512-en-NEN-7513-afgekocht-door-VWS.htm) toe.[[9]](#footnote-9)
* Voor de verstrekking van gegevens via e-mail wordt gebruik gemaakt van een beveiligde emailverbinding.
* Koninklijke Visio werkt volgens de ‘[Richtsnoeren beveiliging persoonsgegevens’](https://cbpweb.nl/sites/default/files/downloads/rs/rs_2013_richtsnoeren-beveiliging-persoonsgegevens.pdf) van de Autoriteit Persoonsgegevens en de ‘Praktijkgids patiëntgegevens in de cloud’ van de Autoriteit Persoonsgegevens.
* De identificerende gegevens zijn zoveel als mogelijk gescheiden opgeslagen van de inhoudelijke gegevens, gepseudonimiseerd of versleuteld.
* De standaardinstellingen zijn nee, tenzij (opt-in) in plaats van ja, mits (opt-out), tenzij de wetgeving opt-out toelaatbaar stelt.
* Koninklijke Visio hanteert per verwerking een autorisatieprotocol. Daarin staat welke gegevens door wie/welke (groepen) medewerkers verwerkt kunnen worden en waarom en welke bevoegdheden zij hebben ten aanzien van welke gegevens (inzage, toevoegen, wijzigen, verwijderen).

## Gegevensbescherming door ontwerp en standaardinstellingen bij Digitale Onderwijsmiddelen[[10]](#footnote-10)

De beginselen voor gegevensbescherming door ontwerp en standaardinstellingen voor het Domein Onderwijs zijn vastgesteld door de PO raad en opgenomen in bijlage 2 van dit reglement.

## Gezamenlijke verwerkingsverantwoordelijken

Wanneer twee of meer verwerkingsverantwoordelijken gezamenlijk de doeleinden en middelen van de verwerking bepalen, zijn zij gezamenlijke verwerkingsverantwoordelijken. Zij stellen op transparante wijze hun respectieve verantwoordelijkheden voor de nakoming van de verplichtingen uit hoofde van deze AVG vast, met name met betrekking tot de uitoefening van de rechten van de betrokkene en hun respectieve verplichtingen om de verplichte informatie te verstrekken, door middel van een onderlinge regeling. In de regeling kan een contactpunt voor betrokkenen worden aangewezen.

Uit de bedoelde regeling blijkt duidelijk welke rol de gezamenlijke verwerkingsverantwoordelijken respectievelijk vervullen, en wat hun respectieve verhouding met de betrokkenen is. De wezenlijke inhoud van de regeling wordt aan de betrokkene beschikbaar gesteld.

Ongeacht een dergelijke regeling kan een betrokkene zijn rechten uit de AVG met betrekking tot en jegens iedere verwerkingsverantwoordelijke uitoefenen.

## Register van verwerkingen

Koninklijke Visio houdt een register bij van de verwerkingsactiviteitendie onder haar verantwoordelijkheid plaatsvinden. Dat register bevat in ieder geval de volgende gegevens:

* de naam en de contactgegevens van Koninklijke Visio en eventuele gezamenlijke verwerkingsverantwoordelijken, en van de functionaris voor gegevensbescherming;
* de verwerkingsdoeleinden;
* een beschrijving van de categorieën van betrokkenen en van de categorieën van Persoonsgegevens;
* de categorieën van ontvangers aan wie de Persoonsgegevens zijn of zullen worden verstrekt, onder meer ontvangers in derde landen of internationale organisaties;
* indien van toepassing, doorgiften van Persoonsgegevens aan een derde land of een internationale organisatie, met inbegrip van de vermelding van dat derde land of die internationale organisatie en, in geval van de in artikel 49, lid 1, tweede alinea, van de AVG bedoelde doorgiften, de documenten inzake de passende waarborgen;
* indien mogelijk, de beoogde termijnen waarbinnen de verschillende categorieën van gegevens moeten worden gewist;
* indien mogelijk, een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen.

Het register is in schriftelijke vorm, waaronder in elektronische vorm, opgesteld. Desgevraagd stelt Koninklijke Visio het register ter beschikking van de Autoriteit Persoonsgegevens.

## Medewerking verlenen aan/samenwerken met de Autoriteit persoonsgegevens[[11]](#footnote-11)

Koninklijke Visio en de verwerker en, in voorkomend geval, hun vertegenwoordigers, werken desgevraagd samen met de Autoriteit Persoonsgegevens bij het vervullen van haar taken.

## Gegevensbeschermingseffectbeoordeling (DPIA)

Wanneer een soort verwerking, in het bijzonder een verwerking waarbij nieuwe technologieën worden gebruikt, gelet op de aard, de omvang, de context en de doeleinden daarvan waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen voert Koninklijke Visio vóór de verwerking een beoordeling uit van het effect van de beoogde verwerkingsactiviteiten op de bescherming van Persoonsgegevens. Eén beoordeling kan een reeks vergelijkbare verwerkingen bestrijken die vergelijkbare hoge risico’s inhouden. Bij het uitvoeren van een gegevensbeschermingseffectbeoordeling wordt het advies van de Functionaris voor Gegevensbescherming ingewonnen.

Een gegevensbeschermingseffectbeoordeling is met name vereist in de volgende gevallen:

* indien sprake is van verwerking van Persoonsgegevens met het oog op het nemen van besluiten over specifieke natuurlijke personen, na een systematische en uitgebreide beoordeling van persoonlijke aspecten van natuurlijke personen, die is gebaseerd op geautomatiseerde verwerking, waaronder profilering, en waarop besluiten worden gebaseerd waaraan voor de natuurlijke persoon rechtsgevolgen zijn verbonden of die de natuurlijke persoon op vergelijkbare wijze wezenlijk treffen;
* er sprake is van een grootschalige verwerking van bijzondere categorieën van Persoonsgegevens, zoals gezondheidsgegevens;
* er sprake is van stelselmatige en grootschalige monitoring van openbaar toegankelijke ruimten.

De beoordeling bevat ten minste:

* een systematische beschrijving van de beoogde verwerkingen en de verwerkingsdoeleinden;
* een beoordeling van de noodzaak en de evenredigheid van de verwerkingen met betrekking tot de doeleinden;
* een beoordeling van het eerste lid van dit artikel bedoelde risico's voor de rechten en vrijheden van betrokkenen; en
* de beoogde maatregelen om de risico's aan te pakken, waaronder waarborgen, veiligheidsmaatregelen en mechanismen om de bescherming van Persoonsgegevens te garanderen en om aan te tonen dat aan deze verordening is voldaan, met inachtneming van de rechten en gerechtvaardigde belangen van de betrokkenen en andere personen in kwestie.

Bij het beoordelen van het effect van de door Koninklijke Visio verrichte verwerkingen en met name ter wille van een gegevensbeschermingseffectbeoordeling, wordt de naleving van gedragscodes naar behoren in aanmerking genomen.

Koninklijke Visio vraagt in voorkomend geval de betrokkenen of hun vertegenwoordigers naar hun mening over de voorgenomen verwerking, met inachtneming van de bescherming van commerciële of algemene belangen of de beveiliging van verwerkingen.

Indien nodig verricht Koninklijke Visio een toetsing om te beoordelen of de verwerking overeenkomstig de gegevensbeschermingsefectbeoordeling wordt uitgevoerd, zulks ten minste wanneer sprake is van een verandering van het risico dat de verwerkingen inhouden.

## Voorafgaande raadpleging van de Autoriteit Persoonsgegevens

Wanneer uit een gegevensbeschermingseffectbeoordeling blijkt dat de verwerking een hoog risico zou opleveren indien Koninklijke Visio geen maatregelen neemt om het risico te beperken, raadpleegt Koninklijke Visio voorafgaand aan de verwerking de Autoriteit Persoonsgegevens.

Wanneer de Autoriteit Persoonsgegevens van oordeel is dat de bedoelde voorgenomen verwerking inbreuk zou maken op deze verordening, met name wanneer Koninklijke Visio het risico onvoldoende heeft onderkend of beperkt, geeft de Autoriteit Persoonsgegevens binnen maximaal acht weken na de ontvangst van het verzoek om raadpleging schriftelijk advies aan Koninklijke Visio en in voorkomend geval aan de verwerker, en mag zij al haar bevoegdheden uitoefenen. Die termijn kan, naargelang de complexiteit van de voorgenomen verwerking, met zes weken worden verlengd. Bij een dergelijke verlenging stelt de Autoriteit Persoonsgegevens Koninklijke Visio en, in voorkomend geval, de verwerker binnen een maand na ontvangst van het verzoek om raadpleging in kennis van onder meer de redenen voor de vertraging. Die termijnen kunnen worden opgeschort totdat de Autoriteit Persoonsgegevens informatie heeft verkregen waarom zij met het oog op de raadpleging heeft verzocht.

* Bij de raadpleging verstrekt Koninklijke Visio de nodige informatie zoals benoemd in de AVG. In ieder geval dienen de volgende gegevens te worden verstrekt:
* indien van toepassing, de verantwoordelijkheden van Koninklijke Visio, bij de verwerking betrokken gezamenlijke verwerkingsverantwoordelijken en verwerkers, in het bijzonder ten aanzien van een verwerking binnen een concern;
* de doeleinden en middelen van de voorgenomen verwerking;
* de maatregelen en waarborgen die worden geboden ter bescherming van de rechten en vrijheden van betrokkenen uit hoofde van de AVG;
* de contactgegevens van de functionaris voor gegevensbescherming;
* de gegevensbeschermingseffectbeoordeling ten aanzien van die verwerking;
* alle andere informatie waar de Autoriteit Persoonsgegevens om verzoekt.

## Beveiliging van de verwerking

Rekening houdend met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen, treffen Koninklijke Visio en de verwerker passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen, die, waar passend, onder meer het volgende omvatten:

* de pseudonimisering en versleuteling van persoonsgegevens;
* het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen;
* het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen;
* een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking.

Bij de beoordeling van het passende beveiligingsniveau wordt met name rekening gehouden met de verwerkingsrisico's, met name als gevolg van vernietiging, verlies, wijziging of ongeoorloofde verstrekking van of ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens, hetzij per ongeluk hetzij onrechtmatig.

Het aansluiten bij een goedgekeurde gedragscode of een goedgekeurd certificeringsmechanisme kan worden gebruikt als element om aan te tonen dat de in hoofdstuk bedoelde vereisten worden nageleefd.

Koninklijke Visio en de verwerker treffen maatregelen om ervoor te zorgen dat iedere natuurlijke persoon die handelt onder het gezag van Koninklijke Visio of van de verwerker en toegang heeft tot persoonsgegevens, deze slechts in opdracht van Koninklijke Visio verwerkt, tenzij hij daartoe volgens wet- en regelgeving is gehouden.

## Meldplicht datalekken

### Melding van een inbreuk in verband met persoonsgegevens aan de Autoriteit Persoonsgegevens (datalekken melden aan de AP) en datalekkenregister

Indien een inbreuk in verband met persoonsgegevens heeft plaatsgevonden, meldt Koninklijke Visio dit zonder onredelijke vertraging en, indien mogelijk, uiterlijk 72 uur nadat zij er kennis van heeft genomen, aan de Autoriteit Persoonsgegevens, tenzij het niet waarschijnlijk is dat de inbreuk in verband met persoonsgegevens een risico inhoudt voor de rechten en vrijheden van natuurlijke personen. Indien de melding aan de Autoriteit Persoonsgegevens niet binnen 72 uur plaatsvindt, wordt de vertraging toegelicht (gemotiveerd).

De verwerker informeert Koninklijke Visio zonder onredelijke vertraging zodra hij kennis heeft genomen van een inbreuk in verband met persoonsgegevens.

In de melding aan de Autoriteit Persoonsgegevens wordt ten minste het volgende omschreven of meegedeeld:

* de aard van de inbreuk in verband met persoonsgegevens, waar mogelijk onder vermelding van de categorieën van betrokkenen en persoonsgegevensregisters in kwestie en, bij benadering, het aantal betrokkenen en persoonsgegevensregisters in kwestie;
* de naam en de contactgegevens van de functionaris voor gegevensbescherming of een ander contactpunt waar meer informatie kan worden verkregen;
* de waarschijnlijke gevolgen van de inbreuk in verband met persoonsgegevens;
* de maatregelen die Koninklijke Visio heeft voorgesteld of genomen om de inbreuk in verband met persoonsgegevens aan te pakken, waaronder, in voorkomend geval, de maatregelen ter beperking van de eventuele nadelige gevolgen daarvan.

Indien en voor zover het niet mogelijk is om alle informatie gelijktijdig te verstrekken, kan de informatie zonder onredelijke vertraging in stappen worden verstrekt.

Koninklijke Visio houdt alle inbreuken in verband met persoonsgegevens bij in een overzicht, met inbegrip van de feiten omtrent die inbreuk, de gevolgen daarvan en de genomen corrigerende maatregelen. Die documentatie stelt de Autoriteit Persoonsgegevens in staat de naleving van dit artikel te controleren.

### Melding van een inbreuk in verband met persoonsgegevens aan de betrokkenen (datalekken melden aan de betrokkene)

Wanneer de inbreuk in verband met persoonsgegevens waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen, deelt Koninklijke Visio de betrokkene de inbreuk in verband met persoonsgegevens onverwijld mee.

De bedoelde mededeling aan de betrokkene bevat een omschrijving, in duidelijke en eenvoudige taal, van de aard van de inbreuk in verband met persoonsgegevens en ten minste de in het vorige artikel 8.9.1 bedoelde gegevens en maatregelen.

De mededeling aan de betrokkene is niet vereist wanneer een van de volgende voorwaarden is vervuld:

* Koninklijke Visio heeft passende technische en organisatorische beschermingsmaatregelen genomen en deze maatregelen zijn toegepast op de persoonsgegevens waarop de inbreuk in verband met persoonsgegevens betrekking heeft, met name die welke de persoonsgegevens onbegrijpelijk maken voor onbevoegden, zoals versleuteling;
* Koninklijke Visio heeft achteraf maatregelen genomen om ervoor te zorgen dat het hoge risico voor de rechten en vrijheden van betrokkenen zich waarschijnlijk niet meer zal voordoen;
* de mededeling zou onevenredige inspanningen vergen. In dat geval komt er in de plaats daarvan een openbare mededeling of een soortgelijke maatregel waarbij betrokkenen even doeltreffend worden geïnformeerd.
* Indien Koninklijke Visio de inbreuk in verband met persoonsgegevens nog niet aan de betrokkene heeft gemeld, kan de Autoriteit Persoonsgegevens, na beraad over de kans dat de inbreuk in verband met persoonsgegevens een hoog risico met zich meebrengt, Koninklijke Visio daartoe verplichten of besluiten dat aan een van de in lid 3 van dit artikel, bedoelde voorwaarden is voldaan.

## Afhandeling datalekken

(Vermoedens van) datalekken worden gemeld aan [privacy@visio.org](mailto:privacy@visio.org). De Functionaris voor Gegevensbescherming beoordeelt of het Datalek moet worden gemeld aan de Autoriteit Persoonsgegevens. Als dit het geval is, meldt de Functionaris voor Gegevensbescherming het Datalek binnen 72 uur. Als het Datalek nadelige gevolgen heeft voor cliënten en/of medewerkers, wordt dit onverwijld aan hen gemeld. Zij kunnen dan maatregelen nemen. Dit is bijvoorbeeld als wachtwoorden of pincodes verloren zijn geraakt. De Functionaris voor Gegevensbescherming zorgt ervoor dat maatregelen worden getroffen om de gevolgen van het Datalek te beperken.

# Functionaris voor gegevensbescherming

## Aanstelling van de functionaris voor gegevensbescherming

Koninklijke Visio is wettelijk verplicht om een Functionaris voor Gegevensbescherming aan te stellen. Deze plicht vloeit voort uit het feit dat Koninklijke Visio hoofdzakelijk is belast met grootschalige verwerking van bijzondere categorieën van gegevens, namelijk: gezondheidsgegevens. De Functionaris voor Gegevensbescherming wordt binnen en buiten de organisatie bekend gemaakt en is aangemeld bij de Autoriteit Persoonsgegevens.

Een concern heeft de mogelijkheid om één functionaris voor gegevensbescherming benoemen, mits de functionaris voor gegevensbescherming vanuit elke vestiging makkelijk te contacteren is.

De functionaris voor gegevensbescherming wordt aangewezen op grond van zijn professionele kwaliteiten en, in het bijzonder, zijn deskundigheid op het gebied van de wetgeving en de praktijk inzake gegevensbescherming en zijn vermogen de hieronder bedoelde taken te vervullen. De vereiste expertise en vaardigheden omvatten in ieder geval

* kennis van nationale en Europese privacywet- en regelgeving over gegevensbescherming;
* begrip van de gegevensverwerkingen die de organisatie uitvoert;
* begrip van IT en informatiebeveiliging;
* kennis van de organisatie en de sector waarin die actief is;
* vaardigheden om binnen de organisatie een cultuur van gegevensbescherming te ontwikkelen.

De functionaris voor gegevensbescherming kan een personeelslid van Koninklijke Visio zijn of kan de taken op grond van een dienstverleningsovereenkomst verrichten.

Koninklijke Visio maakt de contactgegevens van de functionaris voor gegevensbescherming bekend en deelt die mee aan de Autoriteit Persoonsgegevens.

De contactgegevens van de functionaris voor gegevensbescherming worden via de gangbare kanalen voor iedereen toegankelijk gepubliceerd

## Positie van de functionaris voor gegevensbescherming

Koninklijke Visio zorgt ervoor dat de Functionaris voor Gegevensbescherming naar behoren en tijdig wordt betrokken bij alle aangelegenheden die verband houden met de bescherming van Persoonsgegevens. Concreet heeft een Functionaris voor Gegevensbescherming onder meer het volgende nodig om de functie in te vullen:

* de actieve steun vanuit het management;
* voldoende tijd om de taken uit te voeren;
* voldoende praktische ondersteuning (budget, faciliteiten en personeel);
* heldere communicatie aan al het personeel over de benoeming van de FG;
* scholing.

Koninklijke Visio ondersteunt de Functionaris voor Gegevensbescherming bij de vervulling van hieronder bedoelde taken door hem toegang te verschaffen tot Persoonsgegevens en verwerkingsactiviteiten en door hem de benodigde middelen ter beschikking te stellen voor het vervullen van deze taken en het in stand houden van zijn deskundigheid.

Koninklijke Visio zorgt ervoor dat de Functionaris voor Gegevensbescherming geen instructies ontvangt met betrekking tot de uitvoering van die taken; de Functionaris voor Gegevensbescherming werkt zelfstandig en onafhankelijk. De Functionaris voor Gegevensbescherming wordt niet ontslagen of gestraft voor de uitvoering van zijn taken en ondervindt geen nadeel van de uitoefening van zijn taak. De Functionaris voor Gegevensbescherming brengt rechtstreeks verslag uit aan de raad van bestuur.

Betrokkenen kunnen met de Functionaris voor Gegevensbescherming contact opnemen over alle aangelegenheden die verband houden met de verwerking van hun Persoonsgegevens en met de uitoefening van hun rechten uit de AVG.

De Functionaris voor Gegevensbescherming is met betrekking tot de uitvoering van zijn taken tot geheimhouding of vertrouwelijkheid gehouden.

De Functionaris voor Gegevensbescherming kan andere taken en plichten vervullen. Koninklijke Visio zorgt ervoor dat deze taken of plichten niet tot een belangenconflict leiden. Om belangenverstrengeling te voorkomen, mag de functionaris voor gegevensverwerking binnen de organisatie niet ook een functie hebben waarin hij het doel en de middelen van een gegevensverwerking bepaalt. Dit kan bijvoorbeeld zo zijn als de functionaris voor gegevensverwerking een managementpositie vervult, zoals hoofd financiën, strategie, marketing, IT of HRM.

## Taken van de functionaris voor gegevensverwerking

De Functionaris voor Gegevensbescherming vervult ten minste de volgende taken:

* Koninklijke Visio en haar werknemers informeren en adviseren over hun verplichtingen uit hoofde van de privacywetgeving;
* toezien op naleving van deze AVG, van andere gegevensbeschermings-bepalingen en van het beleid van Koninklijke Visio met betrekking tot de bescherming van Persoonsgegevens, met inbegrip van de toewijzing van verantwoordelijkheden, bewustmaking en opleiding van het bij de verwerking betrokken personeel en de betreffende audits;
* desgevraagd advies verstrekken met betrekking tot de gegevensbeschermingseffect-beoordeling (DPIA) en toezien op de uitvoering daarvan;
* met de Autoriteit Persoonsgegevens samenwerken;
* optreden als contactpunt voor de Autoriteit Persoonsgegevens inzake met verwerking verband houdende aangelegenheden, met inbegrip van de voorafgaande raadpleging, en, waar passend, overleg plegen over enige andere aangelegenheid.
* Onderhoudt register met verwerkingsactiviteiten

De Functionaris voor Gegevensbescherming houdt bij de uitvoering van zijn taken naar behoren rekening met het aan verwerkingen verbonden risico, en met de aard, de omvang, de context en de verwerkingsdoeleinden.

## Klachten

Bij een klacht over de naleving van dit reglement kunnen cliënten, leerlingen en medewerkers zich wenden tot de Functionaris voor Gegevensbescherming van Koninklijke Visio via telefoonnummer 088-5855777 of via e-mail: privacy@visio.org.

Betrokkenen hebben ook het recht om een klacht in te dienen bij de Autoriteit Persoonsgegevens.

Voor andere klachten dienen betrokkenen de reguliere klachtenprocedure te volgen.

# Wijzigingen en inzage van dit reglement

De centrale medezeggenschapsorganen (COR, GMR en CCR) hebben instemmingsrecht over het privacyreglement. Koninklijke Visio heeft het recht dit privacyreglement aan te passen. In het geval van relevante en specifieke aanpassingen van het privacyreglement worden deze besproken met de centrale medezeggenschapsorganen.

Dit reglement gaat in per juli 2021 en wordt iedere 2 jaar geëvalueerd. Het meest actuele privacyreglement is in te zien via intranet.

# Bijlage 1 - Begripsbepalingen

In dit reglement wordt verstaan onder:

|  |  |
| --- | --- |
| Autoriteit Persoonsgegevens (AP): | de toezichthoudende autoriteit, de onafhankelijke instantie die erover waakt dat Persoonsgegevens zorgvuldig en veilig worden verwerkt en zo nodig sancties kan opleggen als dat niet gebeurt. |
| Bestand | elk gestructureerd geheel van Persoonsgegevens die volgens bepaalde criteria toegankelijk zijn. |
| Betrokkene: | degene op wie een persoonsgegeven betrekking heeft, meestal de cliënt, of zijn (wettelijk) vertegenwoordiger. |
| Bijzondere categorieën Persoonsgegevens: | Persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid |
| Derde: | elke persoon of instantie die geen betrokkene, verwerkingsverantwoordelijke, verwerker, of een persoon is die onder rechtstreeks gezag van de verwerkingsverantwoordelijke of de verwerker gemachtigd is Persoonsgegevens te verwerken. |
| Functionaris voor Gegevensbescherming (FG): | functionaris die door Koninklijke Visio moet of kan worden aangesteld voor het informeren en adviseren over en het toezicht houden op de toepassing en naleving van de AVG en andere gegevensbeschermingsbepalingen. |
| Gezondheidsgegevens | gegevens over de lichamelijke of geestelijke gezondheid van een persoon, waaronder gegevens over verleende gezondheidsdiensten waarmee informatie over zijn gezondheidstoestand wordt gegeven; |
| Datalek: | een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens. |
| medewerker | alle in de organisatie werkzame personen, waaronder vaste medewerkers, externe (inhuur) krachten, stagiaires, vrijwilligers en leerlingen |
| Persoonsgegevens: | alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon („de betrokkene”); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon. |
| Pseudonimisering: | het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkenen kunnen worden gekoppeld zonder dat aanvullende gegevens worden gebruikt, mits deze aanvullende gegevens apart worden bewaard en technische en organisatorische maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon worden gekoppeld. |
| Toestemming: | door betrokkene, op goede informatie berustende, specifieke, in vrijheid en ondubbelzinnig gegeven toestemming waarbij betrokkene hem betreffende verwerking van Persoonsgegevens aanvaardt. Dat kan door middel van een schriftelijke of mondelinge verklaring of een ondubbelzinnige actieve handeling. |
| Verwerker: | degene die in opdracht van en voor de verwerkingsverantwoordelijke Persoonsgegevens verwerkt |
| Verwerking van Persoonsgegevens | Alle handelingen met betrekking tot Persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of in een andere vorm beschikbaar stellen, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens. |
| Verwerkingsverantwoordelijke: | degene die, alleen of samen met anderen, het doel van en de middelen voor de verwerking van Persoonsgegevens vaststelt; meestal de bestuurder van Koninklijke Visio. |

# Bijlage 2 –Verwerking van persoonsgegevens onderwijs[[12]](#footnote-12)

Voor het domein onderwijs van Visio gelden specifieke privacybepalingen welke zijn opgenomen in het Convenant digitale onderwijsmiddelen en privacy van de PO raad (versie 3.0 – maart 2018). Deze bepalingen zijn in deze bijlage opgenomen en zijn onverkort van toepassing binnen het domein onderwijs van Visio.

## Doeleinden bij verwerking van persoonsgegevens met behulp van leermiddelen en toetsen

De Verwerking van Persoonsgegevens met behulp van Leermiddelen en Toetsen vindt plaats ten behoeve van:

* het met gebruikmaking van het Digitale Onderwijsmiddel geven en volgen van onderwijs en het begeleiden en volgen van Onderwijsdeelnemers, waaronder:
  + de opslag van leer- en toetsresultaten
  + het terugontvangen door de Onderwijsinstelling van leer- en toetsresultaten
  + de beoordeling van leer- en toetsresultaten om leerstof en toetsmateriaal te kunnen verkrijgen dat is afgestemd op de specifieke leerbehoefte van een onderwijsdeelnemer
  + analyse en interpretatie van leerresultaten
  + het kunnen uitwisselen van leer- en toetsresultaten tussen Digitale Onderwijsmiddelen.
* Het geleverd krijgen/ in gebruik kunnen nemen van Digitale Onderwijsmiddelen conform de afspraken die zijn gemaakt tussen de Onderwijsinstelling en de Leverancier;
* Het verkrijgen van toegang tot de aangeboden Digitale Onderwijsmiddelen, en externe informatiesystemen, waaronder de identificatie, authenticatie en autorisatie;
* De beveiliging, controle en preventie van misbruik en oneigenlijk gebruik en het voorkomen van inconsistentie en onbetrouwbaarheid in de, met behulp van het Digitale Onderwijsmiddel Verwerkte, Persoonsgegevens;
* De continuïteit en goede werking van het Digitale Onderwijsmiddel conform de afspraken die zijn gemaakt tussen de Onderwijsinstelling en de Leverancier, waaronder het laten uitvoeren van onderhoud, het maken van een back-up, het aanbrengen van verbeteringen na geconstateerde fouten of onjuistheden en het krijgen van ondersteuning;
* Onderzoek en analyse op basis van strikte voorwaarden, vergelijkbaar met bestaande gedragscodes op het terrein van onderzoek en statistiek, ten behoeve van het (optimaliseren van het) leerproces of het beleid van de Onderwijsinstelling;
* Het door de Onderwijsinstelling voor onderzoeks- en analyse doeleinden beschikbaar kunnen stellen van volledig geanonimiseerde Persoonsgegevens om daarmee de kwaliteit van het onderwijs te verbeteren;
* Het beschikbaar stellen van Persoonsgegevens voor zover noodzakelijk om te kunnen voldoen aan de wettelijke eisen die worden gestel aan Digitale Onderwijsmiddelen;
* De uitvoering of toepassing van een andere wet

## Doeleinden bij verwerking van Persoonsgegevens met behulp van School- en Leerlinginformatiesystemen

De Verwerking van Persoonsgegevens met behulp van School- en Leerlinginformatiesystemen vindt plaats ten behoeve van:

* De organisatie, het geven en volgen van onderwijs, het begeleiden en volgen van Onderwijsdeelnemers of het geven van school- en studieadviezen, waaronder:
  + De indeling en aanpassing van roosters;
  + De analyse en interpretatie van leerresultaten;
  + Het bijhouden van persoonlijke (waaronder medische) omstandigheden van een Onderwijsdeelnemer en de gevolgen daarvan voor het volgen van onderwijs;
  + Het begeleiden en ondersteunen van leerkrachten en andere medewerkers binnen de Onderwijsinstelling;
  + Financieel beheer;
  + Monitoring en verantwoording, ten behoeve van met name: (prestatie)metingen van de Onderwijsinstelling, kwaliteitszorg, tevredenheidsonderzoek, effectiviteitsonderzoek van onderwijs(vorm) of de geboden ondersteuning van Onderwijsdeelnemers bij passend onderwijs;
  + Het behandelen van geschillen;
  + Het uitwisselen van Persoonsgegevens met Derden, waaronder:
    - Toezichthoudende instanties en zorginstellingen in het kader van de uitvoering van hun (wettelijke) taak;
    - Samenwerkingsverbanden in het kader van passend onderwijs, regionale overstappen;
    - Partijen betrokken bij de invulling van stage of leer-/;werkplekken voor zover noodzakelijk en wettelijk toegestaan;
    - Onderwijsinstellingen ingeval van overstappen tussen onderwijsinstellingen en bij vervolgonderwijs.
* Het geleverd krijgen/in gebruik kunnen nemen van Digitale Onderwijsmiddelen conform de afspraken die zijn gemaakt tussen de Onderwijsinstelling en de Leverancier;
* Het verkrijgen van toegang tot de aangeboden Digitale Onderwijsmiddelen, en externe informatiesystemen, waaronder de identificatie, authenticatie en autorisatie;
* De beveiliging, controle en preventie van misbruik en oneigenlijk gebruik en het voorkomen van inconsistentie en onbetrouwbaarheid in de, met behulp van het Digitale Onderwijsmiddel, Verwerkte Persoonsgegevens;
* De continuïteit en goede werking van het Digitale Onderwijsmiddel conform de afspraken die zijn gemaakt tussen de Onderwijsinstelling en de Leverancier, waaronder het laten uitvoeren van onderhoud, het maken van een back-up, het aanbrengen van verbeteringen na geconstateerde fouten of onjuistheden en het krijgen van ondersteuning;
* Onderzoek en analyse op basis van strikte voorwaarden, vergelijkbaar met bestaande gedragscodes op het terrein van onderzoek en statistiek, ten behoeve van het (optimaliseren van het) leerproces of het beleid van de Onderwijsinstelling;
* Het door de Onderwijsinstelling voor onderzoeks- en analyse doeleinden beschikbaar kunnen stellen van volledig geanonimiseerde Persoonsgegevens om daarmee de kwaliteit van het onderwijs te verbeteren;
* Het beschikbaar stellen van Persoonsgegevens voor zover noodzakelijk om te kunnen voldoen aan de wettelijke eisen die worden gesteld aan Digitale Onderwijsmiddelen;
* De uitvoering of toepassing van een andere wet;

De Verwerking van Persoonsgegevens met betrekking tot Digitale Onderwijsmiddelen vindt nooit plaats voor reclamedoeleinden of het doen van ongevraagde aanbiedingen door Leveranciers.

Er vindt door Leveranciers geen verstrekking van Persoonsgegevens aan Derden plaats, tenzij deze uitwisseling plaatsvindt in opdracht van en met instemming van de Onderwijsinstelling of wanneer dit noodzakelijk is om te voldoen aan een eventuele afwijkende Unierechtelijke of lidstaatrechtelijke bepaling op grond waarvan Leverancier tot verstrekken verplicht is, waaronder maar niet beperkt tot het voldoen aan een gerechtelijke uitspraak.

## Gegevensbescherming door ontwerp en standaardinstellingen bij Digitale Onderwijsmiddelen[[13]](#footnote-13)

De beginselen van gegevensbescherming door ontwerp en gegevensbescherming door standaardinstellingen zijn uitgangspunt bij de (door)ontwikkeling van de door Onderwijsinstellingen gebruikte Digitale Onderwijsmiddelen. Binnen het Platform Edu-K worden uitgangspunten en richtlijnen opgesteld hoe hier concreet invulling aan kan worden gegeven, waaronder de mogelijkheid van het toepassen van pseudoniemen.

Onderwijsinstellingen en Leveranciers maken in het kader van de toegang tot en het gebruik van Digitale Onderwijsmiddelen in beginsel gebruik van het Keten iD en de bijbehorende Standaardattributenset. Indien een van de desbetreffende partijen aangeeft dat dit redelijkerwijs niet van haar kan worden gevergd, dient dit voldoende gemotiveerd te worden vastgelegd.

Indien bij algemene maatregel van bestuur voor andere gevallen dan hierboven genoemd besloten wordt tot het gebruik van een nieuw pseudoniem, dan maken partijen binnen het Platform afspraken over het gebruik daarvan.

Partijen zijn gehouden passende technische en organisatorische maatregelen te nemen om ervoor te zorgen dat alleen Persoonsgegevens worden verwerkt die noodzakelijk zijn voor elk specifiek overeengekomen doel van de verwerking.

1. [↑](#footnote-ref-1)
2. Zie artikel 7:456, 7:457 BW (Wgbo). [↑](#footnote-ref-2)
3. In de Wgbo wordt de minderjarigheidsgrens verlaagd van 18 jaar naar 16 jaar. Bij jongeren die de leeftijd van 16 jaar hebben bereikt, is toestemming van de ouders (wettelijk vertegenwoordigers) en het verstrekken van de nodige informatie om toestemming te geven daarom niet nodig, tenzij de betrokkene ter zake wilsonbekwaam is. [↑](#footnote-ref-3)
4. Artikel 7:457, derde lid, BW (Wgbo). [↑](#footnote-ref-4)
5. Zie hiervoor art. 41 UAVG. [↑](#footnote-ref-5)
6. Artikel 457 BW (Wgbo), Dit kan aan de orde zijn als de hulpverlener meent dat het niet in belang van de jeugdige is of als de jeugdige niet wil dat bepaalde informatie wordt verstrekt. [↑](#footnote-ref-6)
7. Er mag slechts informatie worden verstrekt die feitelijk, globaal, belangrijk en doelgericht is. [↑](#footnote-ref-7)
8. Artikel 17, derde lid, AVG (overweging 65). [↑](#footnote-ref-8)
9. Dit in lijn met het besluit elektronische gegevensverwerking door zorgaanbieders. [↑](#footnote-ref-9)
10. De uitgangspunten in deze paragraaf zijn door de PO raad vastgesteld in het convenant Digitale onderwijsmiddelen en privacy – Versie 3.0 – maart 2018. [↑](#footnote-ref-10)
11. Artikel 31 AVG. [↑](#footnote-ref-11)
12. De doeleinden die in deze bijlage zijn vermeld zijn door de PO raad vastgesteld in het convenant Digitale onderwijsmiddelen en privacy – Versie 3.0 – maart 2018. [↑](#footnote-ref-12)
13. De uitgangspunten in deze paragraaf zijn door de PO raad vastgesteld in het convenant Digitale onderwijsmiddelen en privacy – Versie 3.0 – maart 2018. [↑](#footnote-ref-13)