



|  |  |
| --- | --- |
|  |  |
|  | **Toelichting**  **Dataregisters po/vo 2.01** |
|  | ***Dataregister met overzicht van de verwerkingsactiviteiten*** |

**Bron**

Kennisnet

**Colofon**

**Versie** 2.01 (14 november 2018)

**Auteurs** Elly Dingemanse, Ludo Cuijpers (Kennisnet)

**Met dank aan** André Poot (VO-raad), Maurits Huigsloot (PO-Raad)

Job Vos (Kennisnet)

Waar in deze publicatie geschreven wordt in de mannelijke vorm, kan mede de vrouwelijk vorm gelezen worden.

*Hoewel aan de totstandkoming van deze uitgave de uiterste zorg is besteed, aanvaarden de auteur(s), redacteur(s), PO-Raad, VO-raad en Kennisnet geen aansprakelijkheid voor eventuele fouten, onvolkomenheden of schade als gevolg van het gebruik van dit document. Bij twijfel of juridische geschillen wordt geadviseerd om een deskundige in te huren zoals een advocaat, ict-consultant of een in privacy gespecialiseerd jurist.*

Inhoudsopgave

[1 Leeswijzer 4](#_Toc527968824)

[2 Algemene inleiding 5](#_Toc527968825)

[3 Aantoonbaar voldoen aan de AVG 6](#_Toc527968826)

[4 Register van de verwerkingsactiviteiten 8](#_Toc527968827)

[4.1 Welke gegevens bevat het register 8](#_Toc527968828)

[4.2 Format van het dataregister 9](#_Toc527968829)

[4.3 Toelichting opbouw dataregister. 9](#_Toc527968830)

[4.3.1 A: Contactgegevens van de instelling 9](#_Toc527968831)

[4.3.2 B: Categorie van betrokkenen 9](#_Toc527968832)

[4.3.3 C: Verwerkingsdoeleinden 10](#_Toc527968833)

[4.3.4 D: Beschrijving van de categorieën van persoonsgegevens 10](#_Toc527968834)

[4.3.5 E: Brondocumenten 12](#_Toc527968835)

[4.3.6 F + G: Categorieën van verwerkers van persoonsgegevens 12](#_Toc527968836)

[4.3.7 H: Doorgifte van persoonsgegevens buiten de EU 13](#_Toc527968837)

[4.3.8 I: Bewaar- en vernietigtermijnen 13](#_Toc527968838)

[4.3.9 J: Technische en organisatorische maatregelen 14](#_Toc527968839)

[4.3.10 Classificatie van informatie 14](#_Toc527968840)

[5 Het dataregister; de bouwblokken 15](#_Toc527968841)

[5.1 Tabblad 1; het registeroverzicht als praatplaat 15](#_Toc527968842)

[5.2 Tabblad F; andere verwerkingsverantwoordelijken 16](#_Toc527968843)

[5.3 Tabblad G; verwerkers 16](#_Toc527968844)

[5.4 Tabblad X; interne gebruikers 18](#_Toc527968845)

[5.5 Tabblad E, interne documenten 19](#_Toc527968846)

[5.6 Tabblad I; bewaartermijnen 19](#_Toc527968847)

[6 Het vullen van het dataregister 20](#_Toc527968848)

[6.1 Maar waar ga je nu beginnen? 20](#_Toc527968849)

[7 Dataregister als totaaloverzicht 22](#_Toc527968850)

[Bijlage 1: Grondslagen 23](#_Toc527968851)

[Bijlage 2: BIV-classificatie 24](#_Toc527968852)

[Bijlage 3: Ouders informeren 26](#_Toc527968853)

# Leeswijzer

Na de introductie van versie 1.0 zijn de dataregisters voor leerlingen en medewerkers op basis van vragen en opmerkingen vanuit de scholen aangepast. Versie 2.0 is vanaf 10 oktober 2018 beschikbaar.

***Wijzigen ten opzichte van versie 1.0***

* Dataregister voor leerlingen is opgesplitst in een afzonderlijke versie voor po en vo.
* Elk tabblad is voorzien van een korte invulinstructie.
* D.m.v. arceringen zijn invulaanwijzingen per tabblad gegeven.
* Een deel van elk tabblad gaat automatisch naar het registeroverzicht.
* De meest gebruikte verwerkers zijn ingevuld en waar van toepassing van een dropdown menu voorzien.
* Een kort overzicht van de bewaartermijnen is toegevoegd.

Deze toelichting kan gebruikt worden voor alle dataregisters 2.0. De afbeeldingen in dit document komen uit het dataregister leerlingen VO, maar verschillen alleen op detail niveau van de overige registers. Hou bij het lezen van dit document het dataregister digitaal ernaast. Dat helpt om een goed beeld te krijgen van wat het register inhoudt, waar dingen zijn vastgelegd en welke opties er zijn om het optimaal aan te laten sluiten bij de eigen onderwijsinstelling. De **‘LET OP’-**tekstvakken geven extrainformatieen vragen extra aandacht.

Hoofdstuk 3 gaat over het aantoonbaar voldoen aan de AVG.

Hoofdstuk 4 gaat over het register van de verwerkingsactiviteiten, wat daarin moet staan op basis van de AVG en hoe het format dataregister hier invulling aan geeft.

Hoofdstuk 5 geeft een toelichting op de bouwblokken die zijn uitgewerkt in een aantal tabbladen. Deze tabbladen worden kort toegelicht voor wat betreft inhoud, bruikbaarheid en aanpasbaarheid.

Hoofdstuk 6 geeft in 6 stappen aan hoe je het register kan vullen.

Hoofdstuk 7 laat het dataregister als totaaloverzicht zien.

De bijlagen zijn informatief.

Versiebeheer:

|  |  |  |
| --- | --- | --- |
| Versie | Datum | Opmerkingen |
| 2.01 | 14 november 2018 | Naar aanleiding van vragen en opmerkingen vanuit de scholen.  Wijzigingen zijn terug te vinden op tabblad Versiebeheer van de verschillende dataregisters.  Extra aandacht voor de rode tekst op pagina 20 |
|  |  |  |
|  |  |  |

# Algemene inleiding

Onder de Algemene Verordening Gegevensbescherming (AVG) heeft elke onderwijsinstelling en meer expliciet elke verwerkingsverantwoordelijke een verantwoordingsplicht. Onder verwerkings-verantwoordelijken verstaan we alle organisatie, groot of klein, die persoonsgegevens verwerken en daarvoor zelf het doel en de middelen bepalen. Onderwijsinstellingen moeten kunnen aantonen dat ze in overeenstemming met de AVG handelen. Het bijhouden van een register van de verwerkingsactiviteiten (een verwerkingsregister) is vanuit de AVG verplicht. Met een dataregister voldoe je aan de AVG en kun je verantwoording afleggen over wat je met de persoonsgegevens van leerlingen, medewerkers en relaties doet.

Artikel 30 van de AVG geeft aan wat het register van de verwerkingsactiviteiten minimaal moet bevatten. Om aantoonbaar te voldoen aan de AVG moet een school met veel dingen rekening houden en verantwoorden. Het zou makkelijk zijn om vanuit 1 plaats het overzicht te kunnen houden. Daarom is er voor gekozen om naast de wettelijk verplichte onderdelen nog een aantal aanvullende en elkaar overlappende onderwerpen toe te voegen om zo voor het onderwijs een totaaloverzicht te maken. Dit overzicht noemen we het ‘Dataregister’.

Het dataregister bevat onder andere als extra een BIV-classificatie op het niveau van de gebruikte persoonsgegevens, een overzicht van de brondocumenten en de mogelijkheid om aan te geven tot welke persoonsgegevens interne gebruikers toegang hebben (autorisatie) en welke persoonsgegevens er worden opgeslagen in specifieke documenten. Een groot deel van het dataregister is al ingevuld.

Het register van de verwerkingsactiviteiten moet de categorieën van personen van wie gegevens verwerkt worden (de betrokkenen) bevatten. Er is voor gekozen om verschillende dataregisters te maken, die zijn gebaseerd op de categorie van betrokkenen. Dit zijn voor het po en vo een dataregister voor leerlingen po, leerlingen vo, medewerkers po/vo in loondienst, en relaties. Onder relaties vallen onder andere alumni, belangstellenden en sollicitanten. Het register moet actueel gehouden worden. Wanneer er een nieuwe verwerking (intern of extern) plaatsvindt, moet dit in het register worden vastgelegd en/of bijgewerkt.

Het dataregister, en dan met name het overzicht van de verwerkingsactiviteiten, heeft meerdere functies. Het is een verantwoordingsdocument dat moet kunnen worden overhandigd aan de Autoriteit Persoonsgegevens als deze er om vraagt. Het kan ook worden ingezet als de betrokkenen gebruik willen maken van hun privacyrechten. De onderwijsinstelling kan dan relatief snel zien waar welke persoonsgegevens gebruikt worden en met welke instanties deze uitgewisseld worden. Als betrokkenen de school vragen om hun gegevens te corrigeren of te verwijderen, moet dit ook doorgegeven worden aan de organisaties waarmee deze gegevens eventueel worden gedeeld.

Onder de AVG heeft elke organisatie een informatieplicht. Dat betekent dat nieuwe en bestaande leerlingen en medewerkers duidelijk geïnformeerd moeten worden over wat er met hun persoonsgegevens gedaan wordt. In de praktijk is een online privacy toelichting de meest handige manier om hier aan te voldoen. Als de betrokkene meer informatie wilt hebben, dan kan het registeroverzicht op het eerste tabblad als praatplaat gebruikt worden; bijvoorbeeld in de vorm van een flyer op A3 formaat.

# Aantoonbaar voldoen aan de AVG

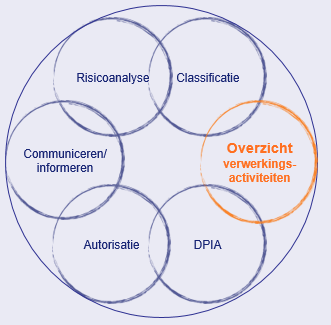
De AVG verplicht organisaties - dus ook scholen - om met passende maatregelen persoonsgegevens die zij verwerken te beschermen. Scholen moeten niet alleen de wet naleven, zij moeten ook kunnen aantonen dat zij zich aan de wet houden.

Scholen hebben een verantwoordingsplicht, ze moeten kunnen aantonen dat de verwerkingen van persoonsgegevens aan de regels van de AVG voldoen. In de AVG zijn een aantal verplichte maatregelen genoemd waarmee aan de verantwoordingsplicht (accountability) kan worden voldaan.

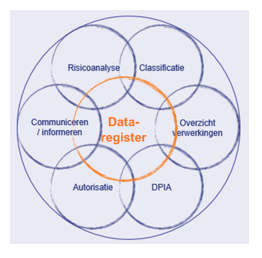
Aantoonbaar voldoen aan de AVG in de praktijk gaat uit van het vastleggen van alles wat je doet met persoonsgegevens. Daarnaast moet je onder andere hierover communiceren richting medewerkers en leerlingen, de uitkomsten van risicoanalyses vastleggen en aangeven in welke mate gegevens belangrijk en/of vertrouwelijk zijn (classificatie.

Maak inzichtelijk wat je doet met persoonsgegevens, wees transparant. En als je dan goed kijkt naar onderstaande tabel, dan hangt alles met elkaar samen.





Een overzicht van de verwerkingsactiviteiten is één van de dingen die organisaties op basis van artikel 30 van de AVG verplicht is om vast te leggen en actueel te houden. Je bent verplicht dit overzicht te laten zien aan de Autoriteit Persoonsgegevens als deze er om vraagt.

Om aantoonbaar te voldoen aan de AVG moet je met veel dingen rekening houden en verantwoorden. Het is dan ook belangrijk om het overzicht houden, het liefst op één plek. Die plek heeft de naam dataregister gekregen.

Het dataregister bevat alle onderdelen, die een register van de verwerkingsactiviteiten moet bevatten én is aangevuld met:

* Overzicht brondocumenten
* Toegang tot persoonsgegevens (autorisatie)
* BIV-classificatie op niveau van gebruikte persoonsgegevens

Het dataregister geeft daardoor:

* inzicht in wat je verwerkt aan persoonsgegevens;
* inzicht in de applicaties die je gebruikt, zowel op de eigen servers als in de cloud (online);
* inzicht in wie toegang heeft tot welke persoonsgegevens;
* een basis voor de autorisatiematrix;
* inzicht in de status van verwerkersovereenkomsten;
* handvatten voor de DPIA en vanuit de DPIA weer de input voor het register; *Zie voor meer informatie over de DPIA de handreiking PDIA van Kennisnet.*
* handvatten om praktisch met de rechten van de betrokkenen om te gaan (bv bij het doorgeven van gegevensaanpassingen aan derden) *Zie voor meer informatie over rechten betrokkenen de handreiking rechten betrokkenen in het po/vo van Kennisnet.*
* Overzicht persoonsgegevens die worden opgeslagen in interne applicaties en specifieke documenten

Bij het verwerken van persoonsgegevens zijn verschillende rollen te onderscheiden namelijk:

* *Betrokkenen*; degene van wie de gegevens verwerkt worden
* *Verwerkingsverantwoordelijken*; degene die het doel en de middelen van de verwerking bepaalt
* *Verwerkers*; degene die persoonsgegevens verwerkt in opdracht van de verwerkingsverantwoordelijke (zonder aan zijn rechtstreeks gezag te zijn onderworpen)
* *Interne gebruikers*; degene die binnen de schoolorganisatie betrokken is bij de verwerking van persoonsgegevens op basis van autorisatie.

De dataregisters zijn gemaakt op basis van betrokkenen. Voor het po en vo zijn op dit moment de laatste versies van de dataregisters:

* Leerlingen po 2.01
* Leerlingen vo 2.01
* Medewerkers po/vo 2.01
* Relaties po/vo 1.0

# Register van de verwerkingsactiviteiten

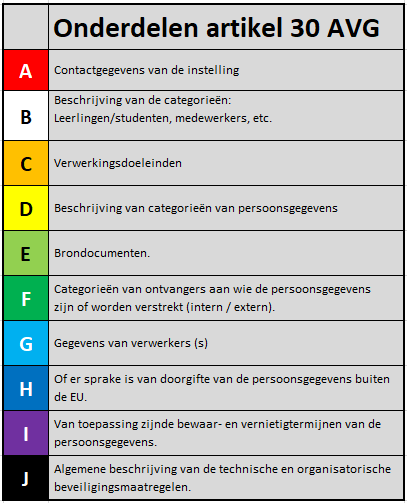
## Welke gegevens bevat het register

De AVG schrijft voor welke informatie er in het register van verwerkingsactiviteiten moet komen te staan. Het register moet minimaal de volgende gegevens bevatten:

* De naam en de contactgegevens van de onderwijsinstelling, de verwerkingsverantwoordelijke en eventuele gezamenlijke verwerkingsverantwoordelijken. Verder de gegevens van de functionaris voor gegevensbescherming en indien van toepassing van de gemandateerde van de verwerkingsverantwoordelijke.
* een beschrijving van de categorieën van personen van wie de gegevens worden verwerkt.

(de categorieën van de betrokkenen);

* opsomming van de categorieën van persoonsgegevens die worden verwerkt;
* de doelen waarvoor deze persoonsgegevens worden verwerkt; de verwerkingsdoeleinden;
* de categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt. Waaronder eventuele andere verwerkingsverantwoordelijke, verwerkers binnen de EU en organisaties in landen buiten de EU (derde landen of internationale organisaties);
* indien mogelijk, de beoogde termijnen waarbinnen de verschillende categorieën van gegevens moeten worden gewist;
* een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen die genomen zijn om de persoonsgegevens, die verwerkt worden, te beveiligen zoals bedoeld in [artikel 32](http://www.privacy-regulation.eu/nl/artikel-32-beveiliging-van-de-verwerking-EU-AVG.htm), lid 1 van de AVG;

De verplichte onderdelen voor het register van de verwerkingsactiviteiten is uitgebreid met o.a. de BIV-classificatie, de brondocumenten en de toegang tot persoonsgegevens door interne medewerkers (autorisatie) en de verwerking ervan in interne documenten.

Het totaaloverzicht dat zo ontstaat noemen we het **dataregister**.

In het dataregister zijn de onderwerpen op basis van artikel 30 van de AVG met kleuren aangegeven zoals in de tabel rechts.

Het is goed om te weten dat het verwerken van persoons-gegevens een zeer ruim begrip is. Onder verwerken wordt in ieder geval het volgende verstaan.

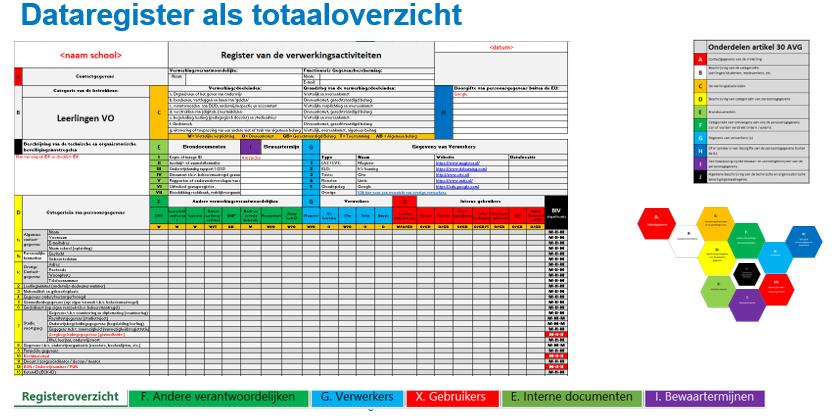
***Verwerken*** *is het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, doorzenden, verspreiden, beschikbaar stellen, samenbrengen, met elkaar in verband brengen, afschermen, uitwissen en vernietigen van gegevens.*

## Format van het dataregister

Er is voor gekozen om het dataregister op basis van de betrokkenen te maken. Het is belangrijk om te weten dat de betrokkene degene is van wie de persoonsgegevens verwerkt worden. Er zijn op dit moment vier dataregister voor het po/vo, namelijk:

1. leerlingen po 2.0
2. leerlingen vo 2.0
3. medewerkers po/vo 2.0
4. relaties 1.0

Alle dataregisters hebben dezelfde opbouw, waarbij de kleuren overeenkomen met de onderdelen uit artikel 30 van de AVG. Het registeroverzicht op het eerste tabblad kan als ‘praatplaat’ gebruikt worden om te laten zien hoe de verwerkingen worden vastgelegd. Het registeroverzicht wordt grotendeels gevuld vanuit de overige tabbladen (zie 4.3). Op het overzicht zijn alleen de witte velden in te vullen.



## Toelichting opbouw dataregister.

### A: Contactgegevens van de instelling

Linksboven kan het logo van de school geplaatst worden en rechtsboven de datum en eventueel de versie van het document. In het witte valk naast contactgegevens vul je de contactgegevens van de verwerkingsverantwoordelijke (het bevoegd gezag, de bestuurder) in. Daarnaast kan eventueel ook de naam van de persoon die door het bevoegd gezag gemandateerd is worden vastgelegd. Van belang is dat ook de gegevens van de Functionaris voor Gegevensbescherming (FG) zijn ingevuld. Zorg dat de FG in ieder geval bereikbaar is via e-mail en eventueel via een contactformulier op de website van de school.

### B: Categorie van betrokkenen

De categorie van betrokkenen staat vermeld bij **B.**

Het dataregister voor leerlingen bevat ook verwerkingen van gegevens van ouders en/of voogden, zoals bij de categorieën persoonsgegevens zijn vermeld. Dit heeft te maken met het feit dat ouders en/of voogden verantwoordelijk zijn voor de privacy van hun kind als deze jonger is dan 16 jaar.

### C: Verwerkingsdoeleinden

Voor het po en vo wordt uitgegaan van de volgende **verwerkingsdoeleinden** :

a. Organisatie of het geven van onderwijs (w.o. onderwijsovereenkomst)

b. Berekenen, vastleggen en innen van ‘gelden’

c. Verantwoorden aan DUO, inspectie en accountant

d. Verstrekken van (digitale) leermiddelen

e. Begeleiding leerling (pedagogisch dossier\*) en studieadvies

f. Onderzoek

g. Uitvoering of toepassing van een andere wet of taak van algemeen belang

\* Pedagogisch dossier bevat o.a. gegevens over voortgang, examineren en aanwezigheid registratie.

Bij alle categorieën van persoonsgegevens is aangegeven voor welke verwerkingsdoeleinden deze gebruikt (kunnen) worden. Een categorie van persoonsgegevens kan voor meerdere doeleinden gebruikt worden. Dit is terug te vinden in de linker kolom (C) van de meeste tabbladen.

***LET OP: Het blijft de verantwoordelijkheid van de onderwijsinstelling om dit voor de eigen situatie te controleren en eventueel aan te passen.***

Naast deze verwerkingsdoeleinden zijn ook de **grondslagen** van belang. Elke verwerking moet ten minste voldoen aan één van de in de wet genoemde *rechtvaardigheidsgronden*, of wel grondslagen. De zes grondslagen vanuit de AVG zijn:

1. Wettelijke verplichting
2. Uitvoering van een overeenkomst

GB. Gerechtvaardigd belang

AB. Algemeen belang (Publiekrechtelijke taak)

1. Vitaal belang
2. Toestemming

In het format zijn in het overzicht bij alle verwerkingen (a t/m g) de grondslagen al aangegeven.

*Bijlage 1* geeft een verdere toelichting van de zes grondslagen.

### D: Beschrijving van de categorieën van persoonsgegevens

Bij .D. worden de categorieën van persoonsgegevens vermeld. Onderstaande tabel geeft, waar nodig, een toelichting op de categorieën persoonsgegevens, die zijn opgenomen in het dataregister.

|  |  |  |  |
| --- | --- | --- | --- |
| **D** | **Categorieën van persoonsgegevens** | | **Omschrijving** |
| **1a** | Algemene contact- gegevens | Naam | Familienaam leerling |
| Voornaam | Voornaam of -namen leerling (incl. voorletters) |
| E-mailadres | E-mailadres leerling |
| Naam school (opleiding) | Naam van de school waar de leerling momenteel onderwijs volgt, eventueel aangevuld met locatienaam |
| **1b** | Persoonlijke kenmerken | Geslacht | Geslacht van de leerling |
| Geboortedatum | Geboortedatum van de leerling |
| **1c** | Overige Contact- gegevens | Adres | Woon- of verblijfadres van de leerling |
| Postcode | Postcode behorende bij het woon- of verblijfadres van de leerling |
| Woonplaats | Woonplaats behorende bij het woon- of verblijfadres van de leerling |
| Telefoonnummer | Telefoonnummer(s) waarop de leerling te bereiken is, zowel mobiel als vaste nummers |
| **2** | Leerlingnummer (onderwijs-deelnemer-nummer) | | Administratienummer dat door de school aan de leerling wordt toegekend |
| **3** | Nationaliteit en geboorteplaats | | Nationaliteit en geboorteplaats van de leerling |
| 4 | Gegevens ouders/verzorger/voogd | | Contactgegevens van de ouders/verzorgers van leerlingen (naam, voornaam, adres, postcode, woonplaats, telefoonnummer en eventueel e-mailadres) |
| **5** | Gezondheidsgegevens (op eigen verzoek t.b.v. beheersmaatregel) | | Gegevens die noodzakelijk zijn met het oog op de gezondheid of het welzijn van de leerling, voor zover deze van belang zijn bij het nemen van aanvullende maatregelen om goed onderwijs te kunnen volgen (bv. extra tijd bij toetsen) |
| **6** | Godsdienst (op eigen verzoek t.b.v. beheersmaatregel) | | Gegevens betreffende de godsdienst of levensovertuiging van de leerling, voor zover die noodzakelijk zijn voor het te volgen onderwijs (bijvoorbeeld: leerling vrij op bepaalde dag). |
| **7** | Studie- voortgang | Gegevens t.b.v examinering en diplomering (examinering) | Gegevens met betrekking het organiseren en afnemen van examens en het opstellen en verstrekken van diploma's |
| Resultaatgegevens (studietraject) | Gegevens met betrekking tot de resultaten die door de leerling behaald zijn, denk aan (rapport)cijfers, beoordelingen, etc. |
| Onderwijsbegeleidingsgegevens (begeleiding leerling) | Gegevens met betrekking tot de voortgang van het leerproces van de leerling, denk aan OPP, observaties, evaluatiegesprekken |
| Gegevens m.b.t. aanwezigheid (aanwezigheidsregistratie) | Gegevens met betrekking tot de aan- en afwezigheid van de leerling en de redenen van afwezigheid |
| Zorgbegeleidingsgegevens (gezondheids-) | Gegevens met betrekking tot het lichamelijk of geestelijk vermogen van de leerling die relevant zijn voor het onderwijs |
| Klas, leerjaar, onderwijssoort | Naam de klas, het leerjaar en het type onderwijs dat de leerling volgt (vmbo, havo, vwo, etc.) |
| **8** | Gegevens t.b.v. onderwijsorganisatie (roosters, boekenlijsten, etc.) | | Gegevens met het oog op het organiseren van het onderwijs en het verstrekken of ter beschikking stellen van leermiddelen; hieronder vallen ook lesroosters, boekenlijsten, schoolpasjes enz. |
| **9** | Financiële gegevens | | Gegevens voor het berekenen, vastleggen en innen van inschrijvingsgelden, school- en/of lesgelden, bijdragen of vergoedingen voor leermiddelen en buitenschoolse activiteiten. (denk hierbij aan een bankrekeningnummer van de ouders) |
| **10** | Beeldmateriaal | | Foto’s en videobeelden (met of zonder geluid) van activiteiten van de school op basis van toestemming. Let op: Voor pasfoto voor identificatiedoeleinden is geen toestemming nodig (schoolpas en als aanvulling op het dossier). |
| **11** | Docent / zorgcoördinator / decaan / mentor | | Gegevens van docenten en begeleiders van de leerling, voor zover deze gegevens van belang zijn voor de organisatie van de instelling en het geven van onderwijs, opleidingen en trainingen |
| **12** | BSN / Onderwijsnummer / PGN | | In het onderwijs heet het BSN het persoonsgebonden nummer (PGN). Ook wel onderwijsnummer genoemd. Het PGN is hetzelfde nummer als het BSN. Scholen zijn verplicht het PGN te gebruiken in hun administratie. |
| **13** | Keten-ID (ECK-ID) | | Unieke ID voor de 'educatieve content-keten'. Hiermee kunnen scholen gegevens delen, zonder dat ze direct herleidbaar zijn naar leerlingen of docenten. |
| **14** | Overige gegevens | | Andere dan de onder 1 tot en met 13 bedoelde gegevens waarvan de verwerking wordt vereist of noodzakelijk is met het oog op de toepassing van een andere wet. Wel moet worden vermeld om welke gegevens het gaat. |

### E: Brondocumenten

De brondocumenten onder .E. zijn de documenten, die als basis gebruikt worden voor het vastleggen van persoonsgegevens van leerlingen en/of medewerkers. Deze gegevens kunnen direct van de betrokkenen verkregen zijn of indirect via een andere persoon, instantie of openbare bronnen. *Zie bijlage 3 voor extra informatie.*

***LET OP:*** *Als er nog andere brondocumenten gebuikt worden, dan kan dat per onderwijsinstelling aangevuld worden. Let daarbij ook op de bewaartermijnen van deze documenten.*

|  |  |
| --- | --- |
|  | **Brondocumenten E** |
| **I** | Kopie of inzage id/paspoort of DigID |
| **II** | Inschrijf- of aanmeldformulier |
| **III** | Overdrachtsformulier, Onderwijskundig rapport (OKR) / OSO |
| **IV** | Document t.b.v. beheersmaatregel gezondheid |
| **V** | Rapporten of onderzoeksverslagen van medische of onderwijskundige specialisten |
| **VI** | Uittreksel gezagsregister |
| **VII** | Beschikking rechtbank, verblijfsvergunning |

*Voorbeeld leerlingen vo*

### F + G: Categorieën van verwerkers van persoonsgegevens

Onderwijsinstellingen verwerken zelf persoonsgegevens, wisselen deze uit met andere organisaties en/of laten andere organisaties in hun opdracht gegevens verwerken. Denk hierbij aan de verplichte uitwisseling van leerlinggegevens met DUO, het laten verwerken van gegevens in de Elektronische leeromgeving (ELO) of het leerling administratiesysteem. Maar ook de interne gebruikers van de onderwijsinstelling vallen hieronder, denk daarbij aan de afdeling PR, de leerling administratie en de medewerkers die toegang hebben tot de zorgbegeleidingsgegevens.

Voor het dataregister worden daarom drie categorieën onderscheiden in te weten:

***Andere verwerkingsverantwoordelijken****,* ***verwerkers*** *en* ***interne gebruikers (autorisatie)*.**

In het dataregister zijn deze elk op apart tabblad uitgewerkt. Onderstaande tabel geeft nadere toelichting.

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Categorie van verwerkers** | **Omschrijving** | **Aandachtspunten** |
| **F** | Andere verwerkings-  verantwoordelijken | Organisaties die vanuit de onderwijsinstelling persoons-gegevens ontvangen, maar tevens zelf verwerkingsverantwoordelijke zijn voor deze gegevens.  Gegevens zullen meestal worden uitgewisseld op basis van een wettelijke verplichting (grondslag). | Met deze organisaties hoeft géén verwerkersovereen-komst te worden afgesloten. |
| **G** | Verwerkers | Organisaties die in opdracht van de verwerkingsverantwoordelijke persoonsgegevens van leerlingen en/of medewerkers verwerken.  Doel en middelen van de verwerking worden bepaald door de bestuurder. | Met deze organisaties moet de onderwijsinstelling verwerkersovereenkomsten afsluiten.  Dit zijn o.a. uitgeverijen, distributeurs en leveranciers van digitaal lesmateriaal. |
| **X** | Interne gebruikers (i.v.m. autorisatie)  (X staat voor de naam van het schoolbestuur /onderwijsinstelling) | Tot welke gegevens hebben de interne gebruikers van schoolbestuur X toegang. | Welke interne gebruikers (docent, mentor, decaan, afdeling PR enz.) mogen bepaalde gegevens verwerken.  Hier is een ‘raakvlak’ met de autorisatiematrix. |

De bestuurder moet als verwerkingsverantwoordelijke verwerkersovereenkomsten afsluiten met alle partijen (organisaties, uitgeverijen enz.), die in opdracht van de onderwijsinstelling bepaalde persoonsgegevens verwerken.

Van deze verwerkers worden in het dataregister de volgende gegevens vastgelegd:

* Naam verwerker
* Omschrijving van de dienst/product
* Website
* Datalocatie
* *Optioneel:* datum afsluiten overeenkomst en versie
* *Optioneel: Applicatiebeheerder intern*

***LET OP:*** *In het format zijn zowel bij leerlingen als bij medewerkers 5 hoofdgroepen van ‘grote verwerkers’ opgenomen (1 t/m 5). De keuze is mede bepaald door het gebruik en de risico’s bij deze groepen. Ook hier geldt dat deze per onderwijsinstelling kunnen worden aangepast als dat beter aansluit bij de eigen situatie. Kijk hierbij ook naar de eventuele (privacy)risico’s die de onderwijsinstelling loopt bij het gebruik van de applicatie.*

### H: Doorgifte van persoonsgegevens buiten de EU

Als er persoonsgegevens worden doorgegeven buiten een EU-lidstaat, Noorwegen, Liechtenstein of IJsland, dan moet dat apart bij .**H**. vermeld worden.

***LET OP:*** *als er applicaties of app’s gebruikt worden waarvan het moederbedrijf zich buiten een EU-lidstaat bevindt en/of persoonsgegevens daarbuiten opslaat vraagt dat extra aandacht. Meer informatie over verwerkingsovereenkomsten en afspraken met leveranciers en distributeurs van digitaal lesmateriaal is terug te vinden in de Aanpak IBP (* [*http://kn.nu/ibponderwijs*](http://kn.nu/ibponderwijs) *) en het privacyconvenant (* [*https://www.privacyconvenant.nl/*](https://www.privacyconvenant.nl/) *).*

### I: Bewaar- en vernietigtermijnen

Organisaties mogen persoonsgegevens niet voor altijd blijven bewaren. Gegevens mogen niet langer verwerkt worden dan nodig is om het gestelde doel te behalen en moeten bij einde bewaartermijn vernietigd worden. Bij **.I.** staan een aantal bewaartermijnen al ingevuld.

*Zie handreiking bewaartermijnen van Kennisnet voor meer informatie.*

***Tip 1:*** *Splits dossiers en administratie van gegevens op naar verschillende bewaartermijnen, zodat deze gegevens op verschillende momenten eenvoudig bijgewerkt en/of verwijderd kunnen worden.*

***Tip 2:*** *Leg vast wie verantwoordelijk is voor het bewaken van de bewaartermijnen.*

### J: Technische en organisatorische maatregelen

Het dataregister moet een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen bevatten, die de onderwijsinstelling genomen heeft om de persoons-gegevens te beschermen. Bij .**J**. is een voorbeeld opgenomen. Welke technische en organisatorische maatregelen er genomen worden en hoeveel is afhankelijk van de risico’s die je loopt bij de verwerking van bepaalde persoonsgegevens in bepaalde systemen.

Het classificeren van gegevens en/of systemen op basis van beschikbaarheid, integriteit en vertrouwelijkheid (BIV-classificatie) is hiervoor de basis. In *bijlage 2* staan deze betrouwbaarheids- of kwaliteitsaspecten kort met de deelaspecten beschreven.

Het dataregister is tevens een hulpmiddel bij het opstellen van een Data Protection Impact Assessment (DPIA)[[1]](#footnote-1).

Het certificeringsschema voor informatiebeveiliging (Edu-K) helpt onderwijsinstellingen en leveranciers de juiste beveiligingsmaatregelen te nemen in de keten. Verder behoren interne en externe audits tot de mogelijkheden.

Zie ook: [https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/verantwoordingsplicht#wat-moet-er-in-het-register-van-verwerkingsactiviteiten-staan-6137](https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/verantwoordingsplicht)

### Classificatie van informatie

Iedere onderwijsinstelling streeft naar een goede balans tussen het optimaal gebruik maken van ict-middelen enerzijds en het borgen van de beschikbaarheid, integriteit en vertrouwelijkheid van informatie anderzijds. Classificatie geeft een inschatting van de gevoeligheid en het belang van informatie om tot een goed niveau van beveiliging te komen. Niet alle informatie is even vertrouwelijk of hoeft bij een incident even snel weer beschikbaar te zijn. Daarnaast is het niet erg efficiënt of gebruiksvriendelijk om niet vertrouwelijke informatie op dezelfde manier te beschermen als vertrouwelijke informatie.

***Informatie*** betekent in dit verband alle data en gegevens, ongeacht het medium (dus ook papieren documenten) waarop deze opgeslagen worden en ongeacht de presentatie daarvan. Informatie wordt in de praktijk verwerkt binnen één of meerdere onderwijs- en/of bedrijfsprocessen en in één of meer systemen/applicaties. Daarnaast wordt informatie ook uitgewisseld met ‘derden’. Gekozen is voor het begrip “classificatie van informatie”, in lijn met de naam van het vakgebied: “informatiebeveiliging”.

Classificatie van informatie helpt bij:

* het kiezen van de juiste maatregelen die genomen moeten worden om informatie adequaat te beschermen, de integriteit te waarborgen en de beschikbaarheid van systemen en gegevens te optimaliseren;
* het vergroten van inzicht van de medewerkers in de onderwijsinstelling als het gaat over informatie en beveiligingsrisico’s.

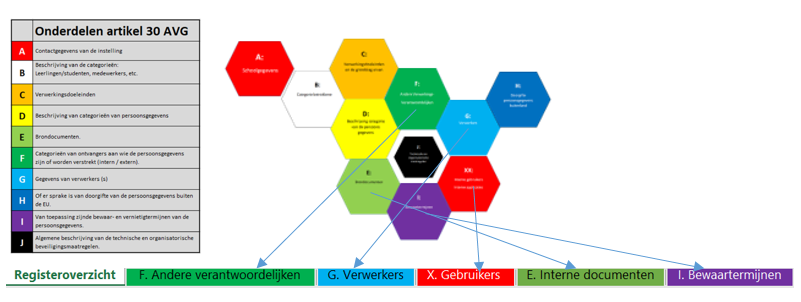
Classificatie draagt ook bij aan:

* een veilige leer- en werkomgeving;
* een goed imago en een veilige school;
* de naleving van wetgeving, waaronder de Algemene Verordening Gegevensbescherming (AVG).

***LET OP:*** *voor het dataregister is op het niveau van categorieën van persoonsgegevens al een classificatie gedaan en zijn de BIV-waarden reeds ingevuld. Merk op dat gezondheidsgegevens, beeldmateriaal en BSN (PGN) op vertrouwelijkheid hoog scoren, dat heeft o.a. consequenties voor de autorisatie.*

# Het dataregister; de bouwblokken

Het dataregister is opgedeeld in bouwblokken. Een groot aantal bouwblokken is inmiddels ingevuld. De overige bouwblokken worden in dit hoofdstuk per tabblad kort toegelicht voor wat betreft inhoud, bruikbaarheid en aanpasbaarheid.



## Tabblad 1; het registeroverzicht als praatplaat

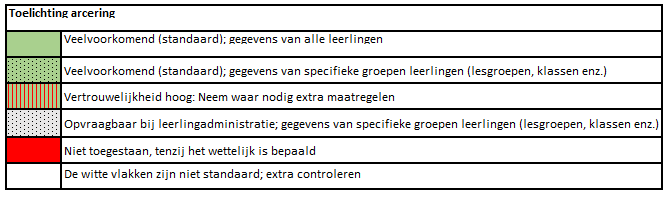
Het registeroverzicht op tabblad 1 is een weergave van de verwerkingsactiviteiten met alle componenten vanuit artikel 30 van de AVG aangevuld met de extra onderwerpen zoals in hoofdstuk 3 zijn aangegeven.



Dit overzicht geeft de mogelijkheid om het gesprek aan te gaan met ouders en/of leerlingen en medewerkers die meer willen weten over het gebruik van hun persoonsgegevens.

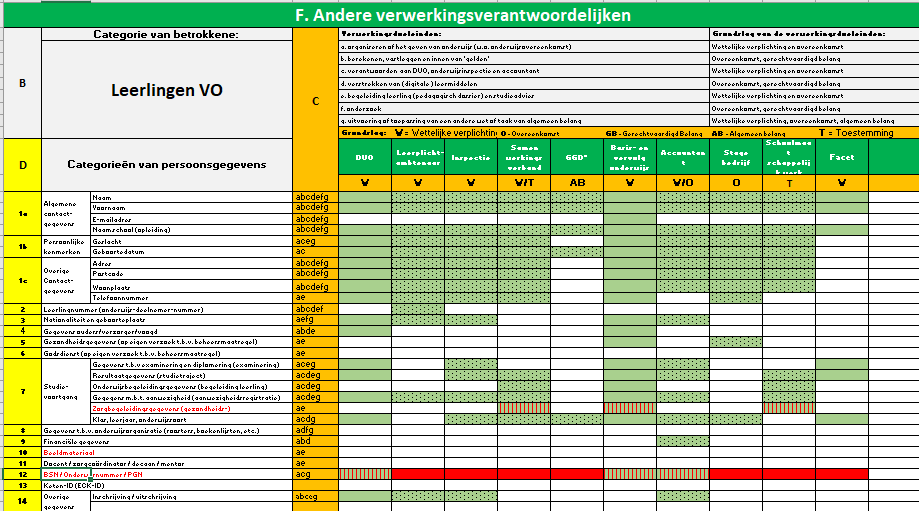
***LET OP:*** *Alleen de witte velden kunnen op het overzicht ingevuld worden. De overige velden worden ingevuld op basis van de tabbladen.*

Vanuit het overzicht kun je er voor kiezen om stapsgewijs het register in te vullen. Elk tabblad is voorzien van een korte invulhulp en een toelichting op de arceringen om het invullen eenvoudiger te maken.



***LET OP:*** *Je moet als school wel zelf de kruisjes zetten in de juiste vakjes. Hierbij is de toelichting bij de arcering van de vakjes een hulpmiddel. Het is en blijft de verantwoordelijkheid van de school om de juiste invulling te geven aan het register.*

## Tabblad F; andere verwerkingsverantwoordelijken



Dit tabblad bevat een overzicht van de ‘andere verwerkingsverantwoordelijke’ dan de eigen onderwijsinstelling.

Na het uitwisselen van de persoonsgegevens zijn die andere verwerkingsverantwoordelijken zelf verantwoordelijk om de privacy van de betrokkenen (degene wiens persoonsgegevens zij ontvangen hebben) te waarborgen.

Het gros van de onderwijsinstellingen wisselt dezelfde categorieën persoonsgegevens met deze instanties uit. Op basis daarvan is de arcering aangebracht in het overzicht. Je kan het overzicht eventueel aanvullen door er een kolom aan toe te voegen.

***LET OP:*** *De onderwijsinstelling blijft altijd zelf verantwoordelijk voor het juist plaatsen van de kruisjes in de al dan niet gearceerde velden.*

***LET OP:*** *De eerste 8 ingevulde verwerkingsverantwoordelijke worden automatisch doorgevoerd naar het overzicht op het eerste tabblad.*

***LET OP:*** *De velden met categorieën van persoonsgegevens op de andere tabbladen verwijzen naar de opsomming dit tabblad.*

## Tabblad G; verwerkers

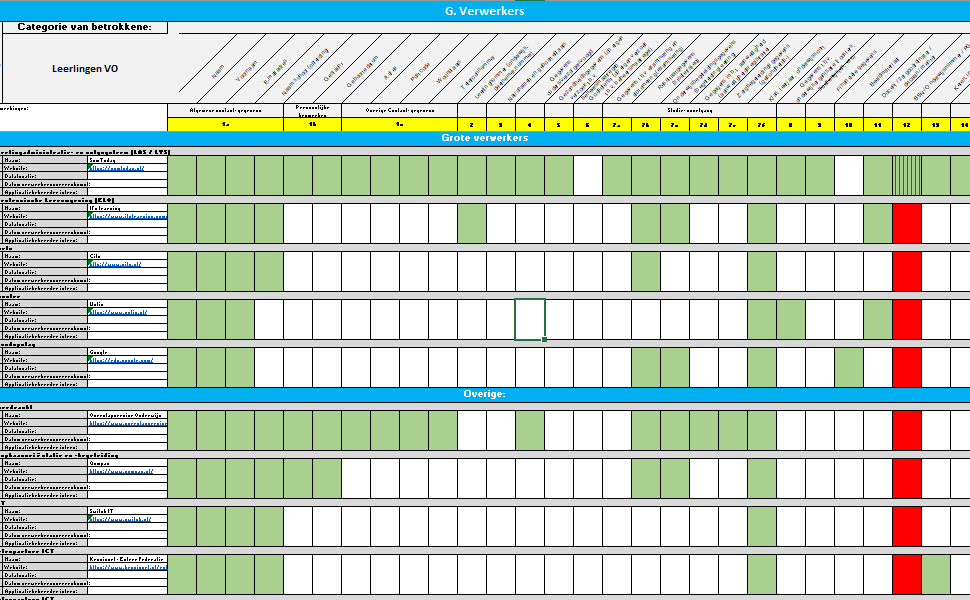
Verwerkers zijn alle organisaties (leveranciers, uitgeverijen en distributeurs ) die in opdracht van de onderwijsinstelling persoonsgegevens verwerken. De onderwijsinstelling (de bestuurder) bepaalt doel en middelen van de verwerking.

Met al deze verwerkers moeten verwerkersovereenkomsten worden afgesloten.

***LET OP:*** *het kan zijn dat van 1 leverancier of uitgever verschillende online pakketten worden afgenomen. De verwerkersovereenkomst moet wel voor elk pakket afgesloten worden. Meestal zal de verwerker zijn geleverde producten in 1 overeenkomst zetten, dit is wel een punt van aandacht.*

In het totaaloverzicht op tabblad 1 zijn de 5 hoofd applicaties opgenomen (1 t/m 5). De keuze is mede bepaald door het gebruik en de risico’s bij deze applicaties.

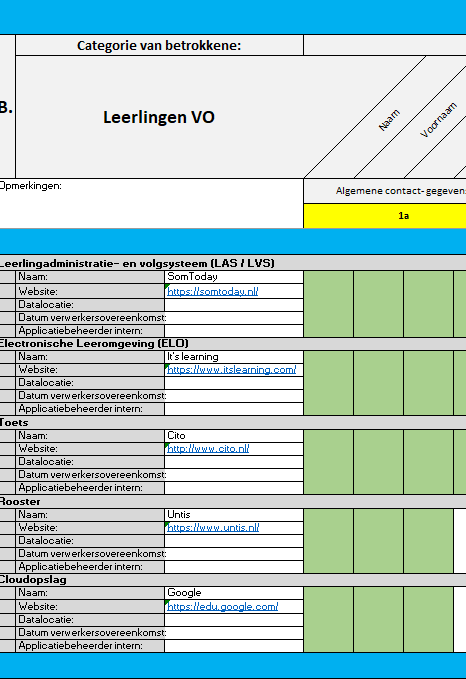
Op tabblad G (Verwerkers) staan deze 5 vermeld onder de blauwe balk met de tekst grote verwerkers.

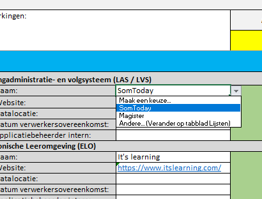


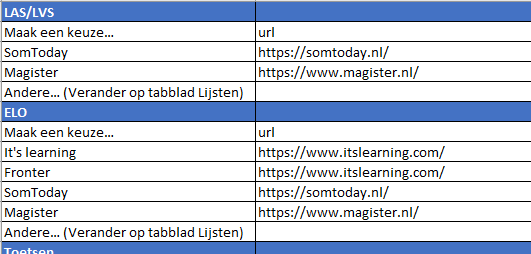
***LET OP****:*

*De ingevulde gegevens van de eerste 5 verwerkers worden automatisch doorgevoerd naar in het overzicht.*

*Hier kunnen géén extra rijen worden toegevoegd, omdat dan de verbinding met het overzicht niet meer klopt!*

Als er van een bepaald systeem meerdere verwerkers zijn wordt er op een aantal plaatsen gebruik gemaakt van een dropdown menu (zie afbeelding hieronder). Hier kun je het systeem kiezen dat je gebruik van maakt.



Staat het systeem dat je gebruikt er niet bij? Kies dan voor ‘andere’ door op het tabblad lijsten bij de regel ‘Andere’ het systeem/pakket in te vullen dat jij gebruikt en vul daarnaast ook de url in.

Schoolbesturen met meerdere scholen gebruiken soms verschillende systemen. Dus naast bijvoorbeeld Magister ook SomToday. Kies dan bij de eerste 5 het systeem (de verwerker) dat het meest gebruikt wordt binnen het bestuur en voeg de andere toe onder de blauwe balk met ‘Overige’.

Verwijder onder de balk ‘Overige’ de verwerkers die je niet gebruikt en vul de lijst aan door het invoegen van steeds een set van 5 regels per systeem, met eventueel een aparte beschrijving erboven.

Onder de balk ‘uitgeverijen en distributeurs staan een groot aantal leveranciers van digitale leermiddelen en educatieve uitgevers. Deze lijst is zeker niet compleet of passend voor elk bestuur, dus pas hem aan zodat hij aansluit bij jouw bestuur.

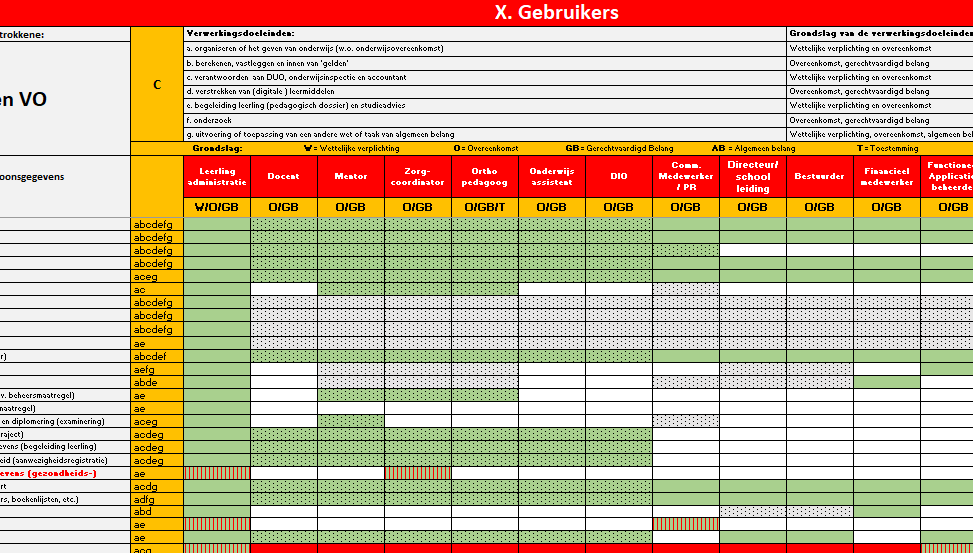
**LET OP:**

*De verwerkersovereenkomsten leveren de input voor dit tabblad. Het is de verantwoordelijkheid van de schoolorganisatie om altijd de gegevens uit de privacybijsluiter te controleren en vervolgens de juiste kruisjes te plaatsen. De arceringen geven alleen een indicatie aan.*

Op tabblad G kan de omschrijving van het pakket, de naam, de website en de datalocatie per verwerker vast worden gelegd. Optioneel kan dit aangevuld worden met de datum van het afsluiten van de verwerkersovereenkomst en de versie ervan. Het is mogelijk om ook per systeem/pakket een interne applicatiebeheerder/ functioneel beheerder en/of eigenaar vast te leggen.

## Tabblad X; interne gebruikers

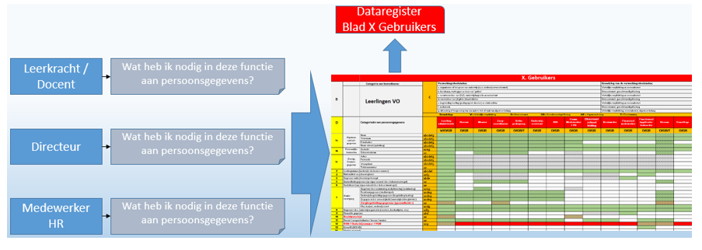
***LET OP:*** *Dit tabblad is niet verplicht vanuit artikel 30 van de AVG, maar geeft wel de mogelijkheid om aan te tonen dat je hebt nagedacht en vastgelegd wie toegang heeft tot welke persoonsgegevens. Als basis voor verdere autorisatie is het dan ook opgenomen in het dataregister.*



Als onderwijsinstelling wissel je niet alleen gegevens uit of laat je anderen in opdracht gegevens verwerken. Ook intern worden er veel persoonsgegevens verwerkt. Dit tabblad laat je nadenken over autorisatie en toegangsminimalisatie. In je IBP-beleid heb je hierover al iets opgenomen.

De AVG verplicht ons om de toegang tot persoonsgegevens te minimaliseren. Je moet medewerkers alleen toegang geven tot die categorieën persoonsgegevens die iemand vanuit zijn functie nodig heeft om zijn werk te doen; om een bepaald doel te bereiken (er is een relatie tussen functie en verwerkingsdoel). Gebruik de onderstaande vraag om invulling aan tabblad X te geven. Bedenk daarbij dat toegang tot persoonsgegevens ook beperkt kan worden tot bepaalde groepen/klassen of alleen opvraagbaar moeten zijn in bepaalde gevallen.

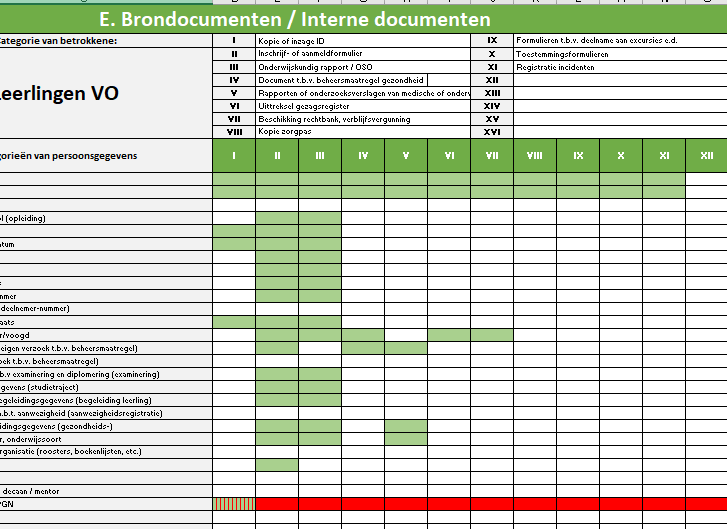
Bepaal en leg vast hoe je dat geregeld hebt. De eerste 8 interne gebruikers worden doorgezet naar het registeroverzicht.



## Tabblad E, interne documenten

Via verschillende brondocumenten krijg je veel persoonsgegevens in je bezit. Op inschrijfformulieren en toestemmingsformulieren en vraag je vaak om (te) veel persoonsgegevens. Al deze gegevens worden vastgelegd in interne documenten. Maar krijg je niet teveel persoonsgegevens binnen of vraag je niet teveel gegevens bij het inschrijven of op een toestemmingsformulier voor een schooluitje?

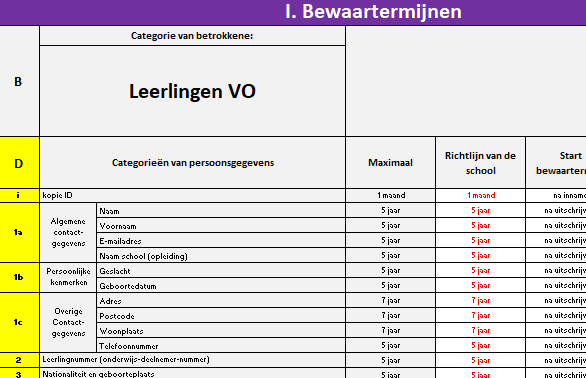
Bijvoorbeeld: *Het vragen om de schoenmaat van een leerling is niet relevant, tenzij je een aantal speciale schoenen moet reserveren voor de excursie. Je moet kunnen onderbouwen waarom je bepaalde gegevens vraagt.*



Op dit tabblad kun je aangeven welke persoonsgegevens de brondocumenten bevatten en wat er in interne documenten wordt vastgelegd.

De invulling van de eerste 7 worden doorgevoerd naar het registeroverzicht.

## Tabblad I; bewaartermijnen



Organisaties mogen persoonsgegevens niet voor altijd blijven bewaren. Gegevens mogen niet langer verwerkt worden dan nodig is om het doel te behalen en moeten bij einde bewaartermijn vernietigd worden.

Bij **.I.** op tabblad 1 staan een aantal bewaartermijnen van de brondocumenten al ingevuld.

Tenzij er een afwijkende reden is voor bewaring moeten persoonsgegevens 2 jaar na beëindiging van de relatie of uitschrijving van de school vernietigd worden. De bewaar- en/of vernietigingstermijn gaat pas lopen nadat de leerling of medewerker de school verlaten heeft (uitgeschreven of uit dienst is). Scholen moeten een overzicht hebben van de relevante bewaartermijnen.

***LET OP:*** *Voor meer informatie zie de handreiking bewaartermijnen van Kennisnet in de Aanpak IBP.*

# Het vullen van het dataregister

Het format dataregister bestaat per betrokkene uit 1 document met verschillende tabbladen. In hoofdstuk 5 zijn deze tabbladen allemaal kort toegelicht en is de aanpasbaarheid en het gebruik ervan beschreven.

## Maar waar ga je nu beginnen?

Veel is er al voor je ingevuld, daar hoef je niet meer over na te denken. In versie 2.0 zijn de volgende aanpassingen gedaan om het starten en invullen eenvoudiger te maken:

* Dataregister voor leerlingen is opgesplitst in een afzonderlijke versie voor po en vo.
* Elk tabblad is voorzien van een korte invulinstructie.
* D.m.v. arceringen zijn invulaanwijzingen per tabblad gegeven.
* Een deel van elk tabblad gaat automatisch naar het registeroverzicht.
* De meest gebruikte verwerkers zijn ingevuld en waar van toepassing is van een dropdown menu voorzien
* Een kort overzicht van de bewaartermijnen is toegevoegd

Dit hoofdstuk laat stap voor stap zien hoe het dataregister gevuld kan worden. Bij elke stap wordt eventueel aangegeven wat er aan voorwerk gedaan moet worden om het invullen zo vlot mogelijk te laten verlopen.

**LET OP:**

*Op basis van input van veel scholen en organisaties zijn de overzichten voorzien van gekleurde aanwijzingen die als* ***richtlijn*** *gebruikt kunnen worden.*

*Het invullen van de tabbladen, het zetten van de definitieve kruisjes, is en blijft de verantwoordelijkheid van het schoolbestuur.*

**Stap 1:**

Begin met het invullen van de witte velden in het registeroverzicht. De grijze velden worden hier automatisch ingevuld vanuit de overige tabbladen en zijn beveiligd.

**Stap 2:**

**Voorwerk:** inventariseer alle organisaties *(andere verwerkingsverantwoordelijke)* waarmee persoonsgegevens van leerlingen en/of medewerkers worden uitgewisseld. (Bijvoorbeeld DUO, leerplicht,  belastingdienst, UWV enz.)

Controleer de rij met andere verwerkingsverantwoordelijken en vul deze desgewenst met een extra kolom aan. Geef met kruisjes of letters aan welke categorieën persoonsgegevens met de verwerkingsverantwoordelijke worden uitgewisseld. Gebruik de gekleurde aanwijzingen als een richtlijn.

De eerste 8 ingevulde kolommen gaan automatisch naar het registeroverzicht.

**Stap 3:**

**Voorwerk:** Inventariseer alle uitgeverijen en distributeurs *(verwerkers)* waarmee persoonsgegevens van leerlingen/medewerkers worden uitgewisseld en pak alle verwerkersovereenkomsten erbij.

De eerste 5 systemen onder de balk ‘grote verwerkers’ zijn gelinkt met het overzicht. Voeg hier dus geen extra rijen aan toe.

Begin met de systemen die hier vermeld staan en maak gebruik van het dropdown menu. Staat het systeem dat je gebruikt er niet bij, maak dan gebruik van de mogelijk om via tabblad lijsten bij ‘andere’ de gewenste verwerker in te vullen. (zie ook 5.3)

**TIP:** *Gebruik je bijvoorbeeld als LAS meer systemen, vul dan onder ‘grote verwerkers’ de meest gebruikte in en voeg een extra set regels toe onder de blauwe balk met ‘overige’ en geeft daar de verwerker van de tweede LAS aan.*

Verwijder de sets van rijen van verwerkers in het overzicht die je niet gebruikt, of geef ze een andere invulling. Vul de reeks van verwerkers aan. Zet de vinkjes op basis van de privacybijsluiter van de verwerkersovereenkomst. Gebruik de arcering als richtlijn.

**Stap 4:**

**Voorwerk:** Inventariseer de functies/rollen om vast te leggen op het tabblad gebruikers.

Controleer de gebruikersgroepen op het tabblad met de groepen die uit het voorwerk komen en pas deze eventueel aan. De eerste 8 ingevulde gebruikersgroepen komen in het registeroverzicht terecht. Zorg ervoor dat hier voor jouw school de belangrijkste groepen staan.

Bepaal tot welke persoonsgegevens de groepen toegang moeten hebben, gebruik de arceringen als een richtlijn.

Op basis van o.a. de input van diverse scholen staat bij de witte vlakken:

*‘Het advies is om medewerkers geen toegang te geven tot gegevens in de witte velden. Besluit je dat bepaalde medewerkers wel toegang moeten hebben, beperk de toegang dan zoveel mogelijk op basis van de verschillende arceringen. De belangrijkste vraag is: Zijn deze gegevens voor de medewerker noodzakelijk om zijn/haar werk te kunnen doen (dataminimalisatie).‘*

Invullen van de witte vlakken is niet verboden, maar vraagt extra aandacht en onderbouwing voor de noodzaak ervan. Alles wat je hier vastlegt vormt de basis voor je autorisatie in documenten, netwerkmappen, applicaties en informatiesystemen.

**Stap 5:**

**Voorwerk:** Inventariseer alle interne formulieren waaronder het inschrijf- of aanmeldformulier, aanmeldingsformulier schoolreis enz.

Controleer de genoemde brondocumenten en interne documenten en wijzig deze of vul ze aan naar behoefte. De eerste 7 worden doorgevoerd naar het registeroverzicht.

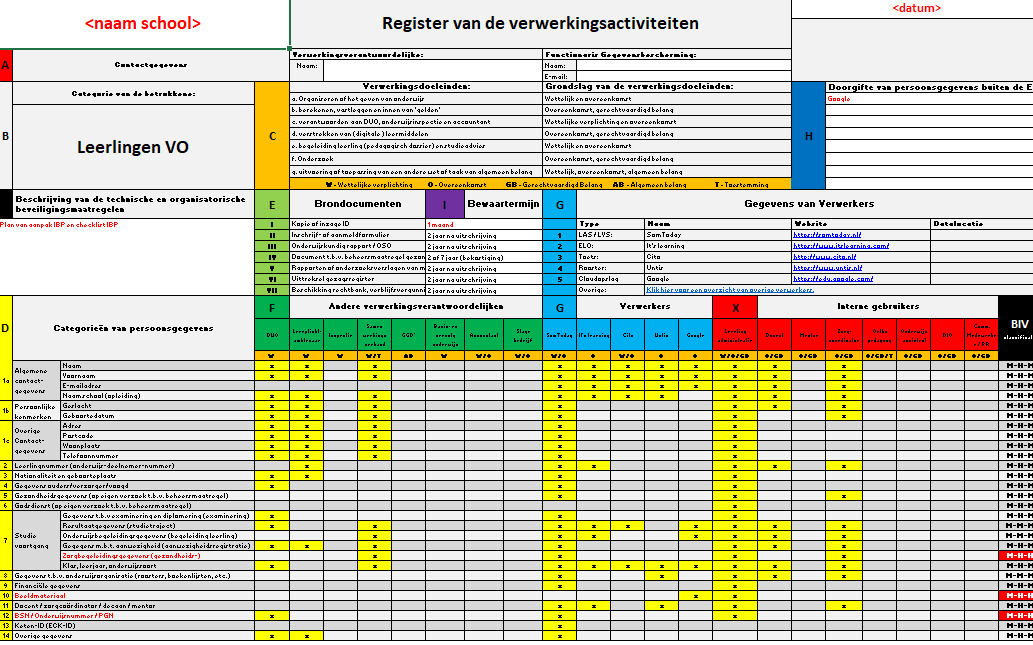
**Stap 6:**

Bekijk de bewaartermijnen die gelden als richtlijn van de school.

# Dataregister als totaaloverzicht

Na stap 6 heb je een voor dat moment actueel register met een ingevuld registeroverzicht op het eerste tabblad. Het dataregister is nooit af. Het is van belang dat het dataregister up-to-date blijft.

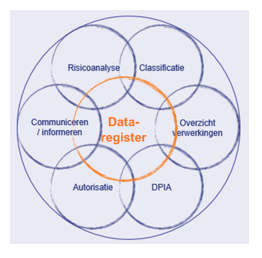
Voer nieuwe verwerkingen direct door in het dataregister.



Voorbeeld

Het dataregister wordt hiermee de plaats voor je totaaloverzicht en geeft je :

* inzicht in wat je verwerkt aan (bijzondere) persoonsgegevens;
* inzicht in de applicaties/informatiesystemen die je gebruikt;
* inzicht in de status van de verwerkersovereenkomsten;
* handvatten voor de DPIA;
* handvatten om praktisch met de rechten van de betrokkenen om te gaan (bv het doorgeven van aanpassingen aan derden);
* inzicht in wie toegang heeft tot welke gegevens; toegangsminimalisatie
* een basis voor de autorisatiematrix



# Bijlage 1: Grondslagen

Toelichting Grondslagen op basis van artikel 6 lid 1 AVG.

|  |  |
| --- | --- |
| **Grondslagen** | **Toelichting** |
| **W: Wettelijke verplichting**  De gegevensverwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op uw organisatie rust | Het gaat om taken die in de wet zijn vastgelegd en die relevant zijn voor uw organisatie. |
| **O: Uitvoering overeenkomst**  De gegevensverwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene een partij is, of om maatregelen te nemen op verzoek van de betrokkene vóór de sluiting van een overeenkomst; | Denk hierbij aan de onderwijsovereenkomst, stageovereenkomst. Alleen die gegevens, die nodig zijn voor de overeenkomst. |
| **GB: Gerechtvaardigd belang**  De gegevensverwerking is noodzakelijk voor de behartiging van een gerechtvaardigd belang van degene die de gegevens verwerkt (of van een derde aan wie de gegevens worden verstrekt). Dit betekent dat degene die de gegevens verwerkt zijn eigen belang moet afwegen tegen het belang en de rechten van de betrokkene. Dit vraagt extra aandacht als betrokkene jonger dan 16 is. Ook moet de verwerker vooraf nagaan of hetzelfde resultaat niet kan worden bereikt met minder gegevens. | Belangrijk om niet te vergeten is dat de betrokkene bezwaar mag maken bij de grondslag gerechtvaardigd belang maar ook wanneer de verwerking plaatsvindt op basis van een publieke taak (artikel 21 AVG). Na een dergelijk bezwaar volgt (opnieuw) een belangenafweging, maar dan op basis van de informatie van het individuele geval. (bv bezwaar tegen de aanschaf van educatieve content)  Zorg ervoor dat u goed kunt onderbouwen dat u zich op deze grondslag mag baseren. |
| **AB: Algemeen belang**  De gegevensverwerking is noodzakelijk 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 uw organisatie is opgedragen | Hierbij heeft de leerling en/of ouders niet het recht om gegevens te (laten) wissen. Wel mag er bezwaar gemaakt worden tegen de verwerking op basis van deze grondslag. |
| **T: Toestemming**  De betrokkene (dit is degene wiens gegevens worden verwerkt) heeft voor de verwerking zijn **ondubbelzinnige** toestemming gegeven voor een of meer specifieke doeleinden. Voor de verwerking van persoonsgegevens van een kind jonger dan 16 jaar is toestemming van een ouder of wettelijk vertegenwoordiger noodzakelijk. Een organisatie moet de verkregen toestemming kunnen aantonen; | Bij de meeste gegevensverwerkingen zal het niet noodzakelijk zijn om toestemming te vragen.  De meeste organisaties kunnen zich baseren op een andere grondslag. Bij het verwerken van bijzondere gegevens kan het zijn dat onder specifieke omstandigheden om uitdrukkelijke toestemming van betrokkene nodig is |
| **VB: Vitaal belang**  De gegevensverwerking is noodzakelijk om de vitale belangen van de betrokkene of van een andere natuurlijke persoon te beschermen | Vitaal belang is een grondslag die niet vaak gebruikt kan worden. Het gaat hierbij echt om levensbedreigende situaties. Is een persoon buiten bewustzijn en is medische hulp noodzakelijk? Dan kunt u zonder toestemming direct de noodzakelijke persoonsgegevens verwerken om hulp te bieden. |

# Bijlage 2: BIV-classificatie

De kwaliteitsaspecten die van toepassing zijn op informatiebeveiliging zijn Beschikbaarheid, Integriteit, en Vertrouwelijkheid. Deze termen worden hier inclusief de deelaspecten beschreven. Alle aspecten kunnen worden geclassificeerd in laag, midden en hoog.

**Beschikbaarheid**

De mate waarin beveiligingsmaatregelen de beschikbaarheid van de informatiesystemen en een ongestoorde voortgang van de ict-dienstverlening waarborgen.

**Midden:** de hersteltijd data is maximaal 24 uur, (netwerk 48 uur).

**Hoog:** de hersteltijd data is maximaal 8 uur, (netwerk 24 uur).

**Integriteit**

De mate waarin de beheersmaatregelen (organisatie, processen en technologie) de volledigheid, juistheid en actualiteit van de informatieverwerking waarborgen.

**Laag:** Volledig; alle gevraagde persoonsgegevens zijn ingevuld. Bijvoorbeeld de postcode (4 cijfers en 2 letters), de geboortedatum (12 januari 1991).

**Midden:** Volledig en Juist; een medewerker van de school controleert of de gegevens juist zijn.

Bijvoorbeeld klopt de naam (controle d.m.v. ID).

**Hoog:** Volledig, juist en actueel, een medewerkers van de school, bijvoorbeeld een medewerker van de leerling administratie, toetst of de leerling nog steeds actief is binnen de school.

**Vertrouwelijkheid**

De mate waarin uitsluitend geautoriseerde personen gebruik kunnen maken van de gegevens of programmatuur, al dan niet gereguleerd door (geautomatiseerde) procedures en/of technische maatregelen.   
Deelaspecten hiervan zijn:

- *Identificatie*: wie bent u;  
- *Authenticatie*: toon aan dat u het bent wie u zegt dat u bent (wachtwoord of pasje);  
- Autorisatie: welke bevoegdheden heeft u;

- Het (geautomatiseerd) vaststellen of geïdentificeerde personen of apparatuur de gewenste handelingen mogen uitvoeren.

- Periodieke controle op de bestaande bevoegdheden.

**Laag:** toegang op basis van de onderwijsovereenkomst (netwerk, e-mail, etc.).

**Midden:** toegang op basis van de rol van de medewerker (bijvoorbeeld: toegang tot aanwezigheidsregistratie).

**Hoog:** toegang alleen op basis van persoonlijke rechten (bijvoorbeeld: een medewerker heeft toegang tot een medisch dossier van de leerling) en extra toegangscontrole

Deelaspecten

**Beschikbaarheid:** de mate waarin beheersmaatregelen de beschikbaarheid en ongestoorde voortgang van de ict-dienstverlening waarborgen.

**Deelaspecten hiervan zijn:**

• Continuïteit: de mate waarin de beschikbaarheid van de ict-dienstverlening gewaarborgd is;

• Portabiliteit: de mate waarin de overdraagbaarheid van het informatiesysteem naar andere gelijksoortige technische infrastructuren gewaarborgd is;

• Herstelbaarheid: de mate waarin de informatievoorziening tijdig en volledig hersteld kan worden.

Voor de beschikbaarheid komt de classificatie laag, midden en hoog respectievelijk overeen met niet vitaal, vitaal en zeer vitaal belang van de gegevens.

**Integriteit:** de mate waarin de beheersmaatregelen (organisatie, processen en technologie) de juistheid, volledigheid en tijdigheid van de IT-dienstverlening waarborgen.

**Deelaspecten hiervan zijn:**

• Juistheid: de mate waarin overeenstemming van de presentatie van gegevens/informatie in IT-systemen ten opzichte van de werkelijkheid is gewaarborgd;

• Volledigheid: de mate van zekerheid dat de volledigheid van gegevens/informatie in het object gewaarborgd is;

• Waarborging: de mate waarin de correcte werking van de IT-processen is gewaarborgd.

Voor de integriteit komt de classificatie laag, midden en hoog respectievelijk overeen met openbaar, intern en vertrouwelijk gebruik van gegevens.

**Vertrouwelijkheid:** de mate waarin uitsluitend geautoriseerde personen, programmatuur of apparatuur gebruik kunnen maken van de gegevens of programmatuur, al dan niet gereguleerd door (geautomatiseerde) procedures en/of technische maatregelen.

**Deelaspecten hiervan zijn:**

• Autorisatie: de mate waarin de adequate inrichting van bevoegdheden gewaarborgd is;

• Authenticiteit: de mate waarin de adequate verificatie van geïdentificeerde personen of apparatuur gewaarborgd is;

• Identificatie: de mate waarin de mechanismen ter herkenning van personen of apparatuur gewaarborgd zijn;

• Periodieke controle op de bestaande bevoegdheden. Het (geautomatiseerd) vaststellen of geïdentificeerde personen of apparatuur de gewenste handelingen mogen uitvoeren.

Voor de vertrouwelijkheid komt de classificatie laag, midden en hoog respectievelijk overeen met openbaar, intern en vertrouwelijk gebruik van gegevens.

**Meer weten over BIV-classificatie zie de Aanpak van Kennisnet.** ( <http://kn.nu/ibponderwijs> )

# Bijlage 3: Ouders informeren

In de AVG is vastgelegd dat onderwijsinstellingen leerlingen en/of ouders op de hoogte moet brengen van de verwerking van persoonsgegevens. Voor het moment waarop ouders hierover geïnformeerd worden wordt hier een onderscheid gemaakt in twee situaties. Dit is afhankelijk van het feit of de onderwijsinstelling de gegevens direct van de ouders krijgt of indirect via een andere persoon of organisatie.

**Gegevens direct verkregen van de ouders**

Artikel 13 van de AVG stelt dat wanneer een school persoonsgegevens over ouders en/of leerlingen *direct van de ouder ontvangt*, de ouders gelijktijdig met het geven van de persoonsgegevens informeert over onder andere de volgende punten:

* de identiteit (volledige naam van de onderwijsinstelling) en de contactgegevens van uw onderwijsinstelling, of de vertegenwoordiger van uw onderwijsinstelling;
* indien van toepassing, de contactgegevens van de functionaris gegevensbescherming;
* voor welk doel u de persoonsgegevens verwerkt en de grondslag van de verwerking;
* de verwerkingsdoeleinden waarvoor de persoonsgegevens zijn bestemd, alsook de rechtsgrond van de verwerking;
* indien van toepassing: ontvangers of categorieën van ontvangers aan wie u de persoonsgegevens (mogelijk) verstrekt;
* indien van toepassing: of u voornemens bent de persoonsgegevens te verstrekken aan een derde land of internationale organisatie. En zo ja, om welk land of internationale organisatie het dan zou gaan;
* hoe lang u de persoonsgegevens zult bewaren;
* wat de rechten van leerlingen en/of ouders zijn; en
* indien van toepassing, of de persoonsgegevens gebruikt worden bij het opstellen van profielen van leerlingen en wat hier de gevolgen van zijn.

Het is van belang aan te geven welke gegevens ouders verplicht moeten geven en wat de gevolgen zijn als ouders en/of leerlingen deze gegevens niet verstrekken.

**Gegevens indirect verkregen**

Artikel 14 van de AVG stelt dat wanneer een onderwijsinstelling persoonsgegevens over leerlingen en/of ouders *indirect, via een ander persoon of organisatie, verkrijgt* leerlingen en/of ouders wel op de hoogte moeten worden gebracht dat dit heeft plaatsgevonden. De onderwijsinstelling moet dat binnen een redelijk termijn, maar uiterlijk binnen één maand nadat persoonsgegevens zijn verkregen, melden. De school informeert de betreffende ouders en/of leerlingen over onder andere de volgende punten:

* de identiteit (volledige naam van de onderwijsinstelling) en de contactgegevens van uw onderwijsinstelling, of de vertegenwoordiger van uw onderwijsinstelling;
* indien van toepassing: de contactgegevens van de functionaris gegevensbescherming;
* voor welk doel u de persoonsgegevens verwerkt;
* welke (categorieën van) persoonsgegevens u heeft verkregen;
* van wie/wat u de persoonsgegevens heeft verkregen; *hierbij kan sprake zijn van het verkrijgen van persoonsgegevens van personen, organisaties of openbare bronnen.*
* indien van toepassing: of u voornemens bent de persoonsgegevens te verstrekken aan een derde land of internationale organisatie. En zo ja, om welk land of internationale organisatie het dan zou gaan;
* of u voornemens bent de persoonsgegevens te verstrekken aan een derde land of internationale organisatie. En zo ja, om welk land of internationale organisatie het dan zou gaan (art. 14, eerste lid, sub f AVG);
* hoe lang u de persoonsgegevens zult bewaren;
* wat de rechten van leerlingen en/of ouders zijn; en
* indien van toepassing, of de persoonsgegevens gebruikt worden bij het opstellen van profielen van leerlingen en wat hier de gevolgen van zijn.

Het is van belang aan te geven welke gegevens ouders verplicht moeten geven en wat de gevolgen zijn als ouders en/of leerlingen deze gegevens niet verstrekken.

Uitzondering informatieplicht

onderwijsinstellingen hoeven de ouders en/of leerlingen niet te informeren over de verwerking van indirect verkregen persoonsgegevens indien:

* de leerling en/of ouder al over de informatie beschikt;
* het informeren onmogelijk blijkt of onevenredig veel inspanning zou vergen;
* het verkrijgen of verstrekken van deze gegevens uitdrukkelijk is voorgeschreven bij unie of lid statelijk recht;
* de persoonsgegevens vertrouwelijk moeten blijven vanwege beroepsgeheim of statutair geheimhoudingsplicht.

1. In het Nederlands Gegevensbeschermingseffectbeoordeling [↑](#footnote-ref-1)