Handleiding
Dataregister leerlingen po/vo

Dataregister met overzicht van de verwerkingsactiviteiten

Laat ict werken **voor het onderwijs**

Bron

Kennisnet

Bewerkt door:
<Naam schoolbestuur> , <naam>

Versiebeheer:

Versie	Status	Datum	Naam	Omschrijving

Bijgewerkt :

Datum	Naam	Functie	Aanpassing

Colofon

Versie 1.0 (13 maart 2018)
Auteurs Elly Dingemanse, Ludo Cuijpers (Kennisnet)

Met dank aan Anne Goris (VO-raad), Maurits Huigsloot (PO-Raad)
Job Vos, Geert van der Sluis, Antoon Fens, Robert van Kuijk

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
2 Inleiding 5
3 Register van de verwerkingsactiviteiten 6
3.1 Welke gegevens bevat het register 6
3.2 Format van het dataregister 7
4 Toelichting opbouw dataregister. 8
4.1 A: Contactgegevens van de instelling 8
4.2 B: Categorie van betrokkenen 8
4.3 C: Verwerkingsdoeleinden 8
4.4 D: Beschrijving van de categorieën van persoonsgegevens 9
4.5 E: Brondocumenten 10
4.6 F + G: Categorieën van verwerkers van persoonsgegevens 10
4.7 H: Doorgifte van persoonsgegevens buiten de EU 11
4.8 I: Bewaar- en vernietigtermijnen 11
4.9 J: Technische en organisatorische maatregelen 11
4.9.1 Classificatie van informatie 12
5 Het dataregister opgedeeld in 10 delen (tabbladen) 14
5.1 Tabblad 1 + 2; Het dataregister als praatplaat 14
5.2 Tabblad 3; Verwerkingsverantwoordelijken 14
5.3 Tabblad 4, 5 en 6; Verwerkers 15
5.4 Tabblad 7; Interne verwerking 15
5.5 Tabblad 8 en 9; Autorisaties 16
5.6 Tabblad 10; Bewaartermijnen 17
6 Het vullen van het dataregister 18
7 Informeren van ouders (leerlingen) over de gegevensverwerking 21
7.1 Voorbeeld privacy toelichting omgaan met persoonsgegevens 21
Bijlage 1: Grondslagen 24
Bijlage 2: Bewaartermijnen 25
Bijlage 3: BIV-classificatie 26
Bijlage 4: Ouders informeren 27

1 Leeswijzer

*Lees de handleiding door met 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 extra informatie over bepaalde onderwerpen.*

Hoofdstuk 3 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 4 beschrijft de opbouw van het dataregister leerlingen po/vo op basis van artikel 30 van de AVG en de keuzes die hierbij gemaakt zijn.
Hoofdstuk 5 geeft een toelichting op het dataregister uitgesplitst naar de tabbladen. Dit zijn de werkdocumenten van het dataregister. Elk werkdocument wordt afzonderlijk besproken en voorzien van tips en de mogelijkheid voor aanpassingen per onderwijsinstelling.
Hoofdstuk 6 Geeft stapsgewijs aan hoe aan de slag te gaan met het register en waar te beginnen.

De bijlagen zijn informatief.

2 Inleiding

Onder de Algemene Verordening Gegevensbescherming (AVG) heeft elke onderwijsinstelling en meer expliciet elke verwerkingsverantwoordelijke een verantwoordingsplicht. Onder verwerkings-verantwoordelijken vallen alle organisatie, groot of klein, die persoonsgegevens verwerken en daarvoor zelf het doel en de middelen bepalen. Dit houdt ook in dat onderwijsinstellingen moeten kunnen aantonen dat er in overeenstemming met de AVG wordt gehandeld. Het bijhouden van een register van de verwerkingsactiviteiten (een verwerkingsregister) is een onderdeel van deze verantwoordingsplicht. Het register van de verwerkingsactiviteiten bevat informatie over de persoonsgegevens die binnen of ten behoeve van de onderwijsinstelling worden verwerkt.

Artikel 30 van de AVG geeft aan wat het register van de verwerkingsactiviteiten minimaal moet bevatten. Er is voor gekozen om naast de wettelijk verplichte informatie nog extra onderwerpen toe te voegen om voor het onderwijs een totaaloverzicht te maken. Dit overzicht noemen we het 'Dataregister'. Het dataregister bevat 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 en welke persoonsgegevens er worden opgeslagen in interne applicaties en specifieke documenten (autorisatie).

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 onder andere een dataregister voor leerlingen po/vo (waaronder ook gegevens vallen van ouders en voogden van leerlingen), medewerkers in loondienst, medewerkers niet in loondienst (waaronder ook externe begeleiders) en relaties. Onder relaties vallen onder andere alumni, belangstellenden, sollicitanten et cetera.

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

Het register dient actueel te worden gehouden. Wanneer er een nieuwe verwerking (intern of extern) plaatsvindt, moet dit in het register worden vastgelegd. Als de Autoriteit Persoonsgegevens vraagt om inzage van het register moet dit getoond kunnen worden. Als een bestuur zowel po als vo scholen heeft is het advies om afzonderlijke dataregisters te maken, dus één voor po en één voor vo. Dat houdt het overzichtelijk.

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. In dit document is een voorbeeld opgenomen. Als de betrokkene meer informatie wilt hebben, dan kan tabblad 1 en tabblad 2 als praatplaat gebruikt worden in de vorm van een flyer op A3 formaat.

3 Register van de verwerkingsactiviteiten

3.1 Welke gegevens bevat het register

In de Algemene verordening gegevensbescherming (AVG) zijn een aantal verplichte maatregelen genoemd waarmee aan de verantwoordingsplicht (accountability) kan worden voldaan. Scholen moeten hiervoor op basis van hun verwerkingen verplicht een register van de verwerkingsactiviteiten bijhouden. De AVG schrijft voor welke informatie er in het register moet komen te staan. Als de Autoriteit Persoonsgegevens (AP) daar om vraagt, moet u het register direct kunnen laten zien.
Het register van de verwerkingsactiviteiten, die onder de verantwoordelijkheid van de bestuurder (de verwerkingsverantwoordelijke) plaatsvinden, moet minimaal de volgende gegevens bevatten:

- De naam en de contactgegevens van de onderwijsinstelling, de verwerkingsverantwoordelijke en eventuele gezamenlijke verwerkingsverantwoordelijken. Indien van toepassing de gegevens van de vertegenwoordiger van de verwerkingsverantwoordelijke (de gemandateerde) en van de functionaris voor gegevensbescherming;
- 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, lid 1 van de AVG;

De verplichte onderwerpen voor het register van de verwerkingsactiviteiten is vervolgens uitgebreid met o.a. de BIV-classificatie, de brondocumenten en de toegang tot persoonsgegevens van interne medewerkers en de verwerking ervan in interne applicaties.
Het totaaloverzicht dat zo ontstaat noemen we het **dataregister**.
In het dataregister zijn de onderwerpen op basis van artikel 30 van de AVG samengevat en met kleuren aangegeven zoals in de tabel rechts.

	Onderdelen artikel 30 AVG
A	Contactgegevens van de instelling
B	Beschrijving van de categorieën: Leerlingen/studenten, medewerkers, etc.
C	Verwerkingsdoeleinden
D	Beschrijving van categorieën van persoonsgegevens
E	Brondocumenten.
F	Categorieën van ontvangers aan wie de persoonsgegevens zijn of worden verstrekt (intern / extern).
G	Gegevens van verwerkers (s)
H	Of er sprake is van doorgifte van de persoonsgegevens buiten de EU.
I	Van toepassing zijnde bewaar- en vernietigtermijnen van de persoonsgegevens.
J	Algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen.

Het is goed om te weten dat het verwerken van persoons-gegevens een zeer ruim begrip is. Hieronder 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.*

3.2 Format van het dataregister

Er is voor gekozen om het format dataregister als ‘praatplaat’ te kunnen gebruiken. Hiervoor kan van tabblad 1 en 2 van het dataregister een flyer gemaakt worden, met het overzicht dataregister aan de ene kant en op de achterkant de privacy toelichting. Het format van het dataregister bevat alle onderdelen vanuit artikel 30 van de Algemene Verordening Gegevensbescherming (AVG).
Het format bestaat uit een ‘leeg’ registeroverzicht met daarbij een aantal werkdocumenten waarin alle informatie kan worden vastgelegd. Hierbij wordt de mogelijkheid geboden om in een aantal gevallen te kiezen tussen 2 werkdocumenten. Op deze manier kunnen onderwijsinstellingen het vastleggen van de gegevens afstemmen op de grootte van de instelling. Dit zal bij het invullen van het dataregister in hoofdstuk 5 verder toegelicht worden.

	Logo Onderwijsinstelling																										Dataregister 1
			Register van de verwerkingsactiviteiten (Data register) Artikel 30 AVG																								Versie: 16-2-2018
A	Contactgegevens van XX		Verwerkingsverantwoordelijke:																								
			XX (voorzitter College van Bestuur)																								
			Gemandateerd: XX (Bijvoorbeeld Directeur Bedrijfsvoering)																								
B	Categorie van de berokkene:	C	Verwerkingsdoeleinden:																								
	Leerlingen PO/VO		a. Organiseren of het geven van onderwijs (w.o. onderwijsovereenkomst)																								
			b. berekenen, vastleggen en innen van 'gelden'																								
			c. verantwoorden aan DUO, onderwijsinspectie 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																								
J	Algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen	E	Brondocumenten							I	Bewaartermijnen																
	voorbeeld: Assessment uitgevoerd op de informatiebeveiliging (ISO 27002), beoordeling volwassenheidsniveau 2,5 op basis van Toetsingskader SURF (schaal 1-5). Beoordeling uitgevoerd op Privacy (AVG2018), beoordeling volgt.	I	(Digitaal) aanmeldingsformulier							2 jaar of 7 jaar (bekostiging)																
		II	Kopie of inzage id/paspoort of DigID							Maximaal 1 maand																	
		III	Doc. beheersmaatregel gezondheid							2 jaar of 7 jaar (bekostiging)																	
		IV	Overdrachtsformulier (o.a. OKR, OSO)							2 jaar n.b.o.																	
		V	Specifieke documenten**							2 of 7 jaar n.b.o.																	
		VI																									

G	Gegevens van verwerkers (cloud)			
	naam	omschrijving	Website informatie (vb)	Datalocatie (vb)
1	LAS / LVS: Magister	Studenten Informatie Systeem	www.magister.nl	Hengelo
2	ELO:			
3	Toets:			
4	Rooster:			
5	CRM:			
	Overig	Uitwerking overig en uitgeverijen in verwerkersoverzicht tabblad 5		

D	Categorieën van persoonsgegevens		F	Andere verwerkingsverantwoordelijken									G	Verwerkers					XX	Interne gebruikers				Interne applicaties ----			BIV
			DUO	Leer plicht	school inrp	SWV	Accoun tant	GGD artz	CJP	Stage bedrijf	vervolg onderw	Overig ...	LAS 1	ELO 2	Toets 3	Rooster 4	CRM 5	Overig	leerling Admin.	docent	mentor	decaan	IB-er Zorg	PR overig	ICT IDM	Finan-cien	classificatie
1a	Contactgegevens: naam, e-mail, opleiding																										M-H-M
1b	Contactgegevens: geboortedatum en geslacht																										M-H-M
1c	Contactgegevens: overige gegevens																										M-H-M
2	Leerlingnummer																										M-H-M
3	Nationaliteit en geboorteplaats																										M-H-M
4	Gegevens ouders of voogd																										M-H-M
5	Medische gegevens (op eigen verzoek/vrijwillig)																										M-H-M
6	Godsdienst (op eigen verzoek/vrijwillig)																										M-H-M
7	Studie voortgang	7a Examinering																									M-H-M
		7b Studietraject																									M-M-M
		7c Begeleiding leerling																									M-M-M
		7d Aanwezigheidsregistratie																									M-H-M
		7e Medisch dossier (papier)																									M-H-H
		7f Klas, leerjaar, opleiding																									M-H-M
8	Onderwijsorganisatie (roosters, boekenlijsten, etc.)																										M-M-M
9	Financiën (volledige cyclus)																										M-H-M
10	Beeldmateriaal																										M-H-H
11	Docent/zorgcoördinator/ IB-er/ decaan/ mentor																										M-H-M
12	BSN (PGN)																										M-H-H
13	Eck-ID (keten ID)																										M-H-M
14	Overige gegevens																										M-H-M

4 Toelichting opbouw dataregister.

4.1 A: Contactgegevens van de instelling

Bovenaan naast de rode .A. staan de contactgegevens van de instelling en de naam van de verwerkingsverantwoordelijke (het bevoegd gezag, de bestuurder). Daarnaast kan eventueel ook de naam van de persoon die 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.

4.2 B: Categorie van betrokkenen

De categorie van betrokkenen wordt vermeld bij **B**, in dit geval de leerlingen. Het dataregister voor leerlingen bevat ook verwerkingen van gegevens van ouders en/of voogden, zoals bij de categorieën persoonsgegevens zijn vermeld. Dit heeft onder andere 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.

4.3 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 wordt aangegeven voor welke verwerkingsdoeleinden deze gebruikt (kunnen) worden. Een categorie van persoonsgegevens kan voor meerdere doeleinden gebruikt worden. Dit is steeds terug te vinden in de linker kolom (C) van de meeste werkdocumenten.

LET OP: Het blijft de verantwoordelijkheid van de onderwijsinstelling om dit voor de eigen situatie te controleren en indien nodig 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:

T. Toestemming;
U. Uitvoering van een overeenkomst;
W. Wettelijke verplichting
V. Vitaal belang
P. Publiekrechtelijke taak (taak algemeen belang)
GB. Gerechtvaardigd belang

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.

4.4 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.

Categorie	Toelichting
1. Contactgegevens	**1a:** naam, voornaam, e-mail, opleiding *(bv. sector techniek)*; **1b:** geboortedatum, geslacht; **1c:** overige gegevens te weten: adres, postcode, woonplaats, telefoonnummer en eventueel andere voor communicatie benodigde gegevens, alsmede ook een bankrekeningnummer voor het afhandelen van betalingen**;**
2. Leerling nummer	een administratienummer dat geen andere informatie bevat dan bedoeld onder categorie 1
3. Nationaliteit en geboorteplaats	
4. Ouders, voogd	contact gegevens van de ouders/verzorgers van leerlingen (naam, voornaam, adres, postcode, woonplaats, telefoonnummer en eventueel e-mailadres)
5. Medische gegevens	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	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. Studievoortgang	gegevens betreffende de aard en het verloop van het onderwijs en de behaalde studieresultaten te weten: • Examinering; (gegevens rondom het examen) • Studietraject • Begeleiding leerling (inclusief ontwikkelperspectief OPP) • Aanwezigheidsregistratie • Medisch dossier (papier) • Klas, leerjaar, opleiding
8. Onderwijsorganisatie	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. Financiën	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 /zorgcoördi-nator/ intern begeleider/ decaan / mentor	gegevens van **docenten en begeleiders,** voor zover deze gegevens van belang zijn voor de organisatie van de instelling en het geven van onderwijs, opleidingen en trainingen
12. BSN (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 contentketen'. Hiermee kunnen scholen gegevens delen, zonder dat ze direct herleidbaar zijn naar leerlingen of docenten.
14 Overige gegevens, te weten ….	andere dan de onder 1 tot en met 11 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.**

4.5 E: Brondocumenten

De brondocumenten onder .E. zijn die documenten, die als basis gebruikt worden voor het vastleggen van persoonsgegevens van leerlingen. Deze gegevens kunnen direct van leerlingen en/of ouders verkregen zijn of indirect via een andere persoon, instantie of openbare bronnen.
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	(Digitaal) aanmeldingsformulier
II	Kopie of inzage id/paspoort of DigID
III	Document beheersmaatregel gezondheid
IV	Overdrachtsformulier (o.a. OKR, OSO)
V	Specifieke documenten (eventuele rapporten (dyslexie, psycholoog, etc.), verblijfsvergunning, ontheffing en toestemmingsformulieren)
VI	

4.6 F + G: Categorieën van verwerkers van persoonsgegevens

Onderwijsinstellingen verwerken 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 medische dossiers.

Voor het dataregister worden drie categorieën onderscheiden in te weten:
Andere verwerkingsverantwoordelijken, ***verwerkers*** *en* ***interne gebruikers.***
Onderstaande tabel geeft nadere toelichting.

	Categorie van verwerkers	**Omschrijving**	**Aandachtspunten**
F	Andere verwerkings-verantwoordelijken	Organisaties die vanuit de onderwijsinstelling persoonsgegevens 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 verwerkersovereenkomst te worden afgesloten.
G	Verwerkers	Organisaties die in opdracht van de verwerkingsverantwoordelijke van de onderwijsinstelling persoonsgegevens verwerken. Doel en middelen van de verwerking worden bepaald door de bestuurder.	Met deze organisaties moeten verwerkersovereenkomsten worden afgesloten. Dit zijn o.a. softwareleveranciers, uitgeverijen en distributeurs.
XX	Interne gebruikers (XX staat voor de naam van het schoolbestuur /de onderwijsinstelling)	De persoonsgegevens die o.a. opgeslagen worden in: • applicaties binnen het eigen netwerk, • leerling dossiers, • inschrijfformulieren • het ontwikkelperspectief (OPP). Maar ook de gegevens waar de interne gebruikers van instelling XX toegang toe hebben en zelf kunnen verwerken.	Hoewel het aantal applicaties dat op eigen servers draait afneemt, is het wel van belang voor die applicaties die nog wel 'intern' draaien te weten welke persoonsgegevens daarin worden vastgelegd. 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:

- Omschrijving van de dienst/product
- Naam verwerker
- Website
- Datalocatie
- *Optioneel:* datum afsluiten overeenkomst en versie (zie tabblad 6)

LET OP: *In het format zijn 5 hoofdgroepen van applicaties 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 het pakket.

4.7 H: Doorgifte van persoonsgegevens buiten de EU

Indien 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) en het privacyconvenant (https://www.privacyconvenant.nl/).*

4.8 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.
Bijlage 2 bevat een (concept)overzicht van de bewaartermijnen, die grotendeels is gebaseerd op de Wet bescherming persoonsgegeven.
Tabblad 10 is een voorbeeld werkdocument om de bewaartermijnen vast te leggen.

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.*

LET OP: *Op dit moment wordt er gewerkt aan een overzicht van bewaartermijnen, waarin ook de archiefwet wordt opgenomen. Zodra deze beschikbaar is zal deze in de Aanpak IBP terug te vinden zijn.*

4.9 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 gegevens in bepaalde systemen. Het classificeren van gegevens en/of systemen op basis van beschikbaarheid, integriteit en vertrouwelijkheid (BIV-classificatie) is hiervoor de basis.

Het dataregister is tevens een hulpmiddel bij het opstellen van een Data Protection Impact Assessment (DPIA) of een Privacy Impact Assessment (PIA)[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

4.9.1 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).

De kwaliteitsaspecten die betrekking hebben op informatiebeveiliging zijn **B**eschikbaarheid, **I**ntegriteit, en **V**ertrouwelijkheid, vandaar de naam **BIV**-classificatie.

Wat classificeren verder inhoudt en hoe je het classificatieniveau kan bepalen is terug te vinden in de Aanpak IBP.
In *bijlage 3* staan deze kwaliteitsaspecten (betrouwbaarheidsaspecten) kort met de deelaspecten beschreven.

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 medische gegevens, beeldmateriaal en BSN (PGN) op vertrouwelijkheid hoog scoren, dat heeft o.a. consequenties voor de autorisatie.*

[1] In het Nederlands Gegevensbeschermingseffectbeoordeling

Onderstaande tabel geeft een beknopte uitleg van de drie aspecten met voorbeeld:

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.

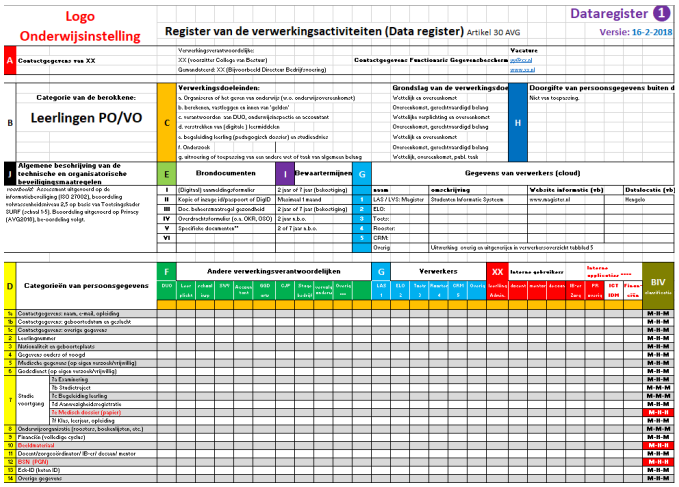
Laag: toegang op basis van de onderwijsovereenkomst (netwerk, e-mail, etc.).
Midden: toegang op basis van de rol van de medewerker (bijvoorbeeld: toegang tot aanwezigheidsregistratie).
Hoog: toegang alleen op basis van persoonlijke rechten (bijvoorbeeld: een medewerker heeft toegang tot een medisch dossier van de leerling) en extra toegangscontrole

5 Het dataregister opgedeeld in 10 delen (tabbladen)

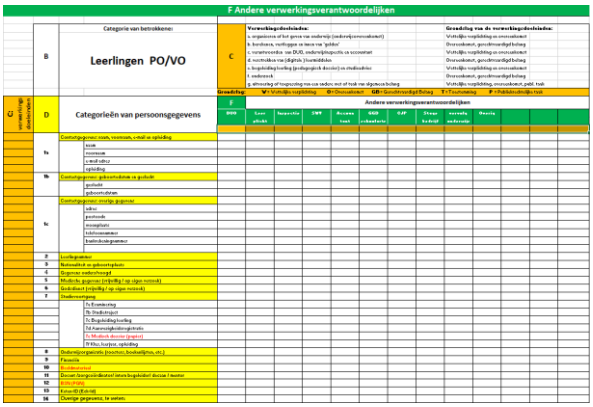
Het dataregister is opgedeeld in een aantal voorbeeld werkdocumenten, die zijn weergegeven in 10 tabbladen. In dit hoofdstuk worden de werkdocumenten kort toegelicht voor wat betreft inhoud, bruikbaarheid en aanpasbaarheid.

5.1 Tabblad 1 + 2; Het dataregister als praatplaat

Het totaaloverzicht 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 is aangegeven.
Deze kan op A3 afgedrukt worden en op de achterkant voorzien worden van de inhoud van tabblad 2, de privacy toelichting.
De ontstane flyer geeft de mogelijkheid om het gesprek aan te gaan met ouders en/of leerlingen, die meer willen weten over het gebruik van hun gegevens. Daarnaast kan de privacy toelichting via de website gepubliceerd worden. Pas de privacy toelichting eventueel aan zodat hij aansluit bij de onderwijsinstelling.



5.2 Tabblad 3; Verwerkingsverantwoordelijken

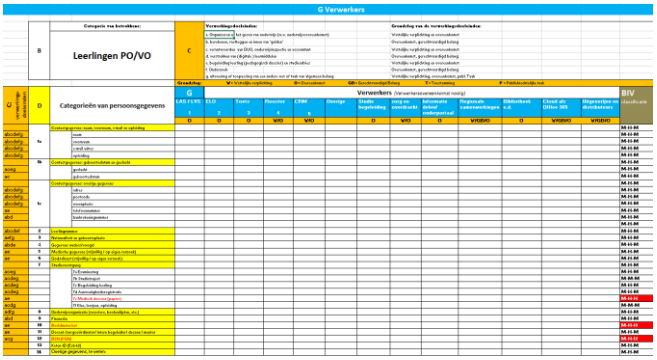


Dit tabblad bevat een overzicht van de ‘andere verwerkingsverantwoordelijke’ dan de eigen onderwijsinstelling.
Na het uitwisselen van de gegevens zijn die andere verwerkingsverantwoordelijken zelf verantwoordelijk om de privacy van de betrokkenen (degene wiens persoonsgegevens zij ontvangen hebben) te waarborgen.
Dit overzicht kan gelijk als werkdocument gebruikt worden. Er is een mogelijkheid om, indien gewenst, op de lege velden uit te breiden en/of aan te passen.

Het ligt in de lijn van de verwachting dat het gros van de onderwijsinstellingen dezelfde categorieën persoonsgegevens met deze instanties uitwisselen. Er wordt dan ook gewerkt aan een ingevuld overzicht.

LET OP: *De onderwijsinstelling blijft altijd zelf verantwoordelijk voor het juist invullen van de gegevens. Een ingevuld overzicht verandert hier niets aan.*

5.3 Tabblad 4, 5 en 6; Verwerkers



Verwerkers zijn alle organisaties (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 uitgeverijen en distributeurs moeten verwerkersovereenkomsten worden afgesloten.

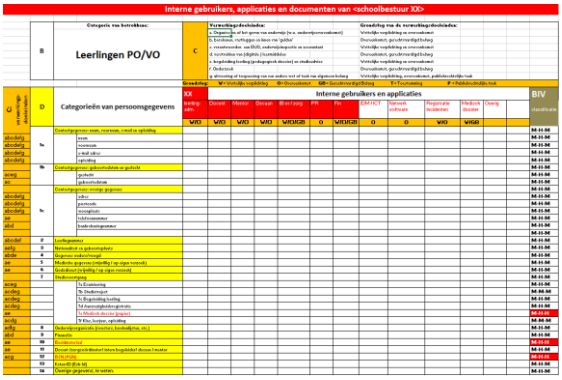
LET OP: *het kan zijn dat van 1 leverancier verschillende online pakketten worden afgenomen. De verwerkersovereenkomst moet wel voor elk pakket afgesloten worden. Meestal zal de verwerker zijn geleverde producten in 1 overeenkomst zetten, maar dit is wel een punt van aandacht.*

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.
In het overzicht op tabblad 4 zijn er al een aantal toegevoegd. Een kleine onderwijsinstelling kan dit schema aanpassen en het gelijk als werkdocument gebruiken. Meestal zal dit niet voldoende zijn en zal zeker de lijst van uitgeverijen en distributeurs uitgebreider zijn.
Tabblad 4 (Verwerkers) kan dan in combinatie met tabblad 5 (Verwerkersoverzicht) gebruikt worden. Tabblad 5 geeft teven de mogelijkheid om per pakket een omschrijving/opmerking te plaatsen en om een functioneel beheerder en/of eigenaar vast te leggen.

Vanuit artikel 30 van de AVG wordt ook gevraagd om gegevens van de verwerkers vast te leggen. Tabblad 6 geeft alle ruimte om de omschrijving van het pakket, de naam, de website voor informatie en de datalocatie vast te leggen. Optioneel kan dit aangevuld worden met de datum van het afsluiten van de overeenkomst en de versie van de overeenkomst.

5.4 Tabblad 7; Interne verwerking

LET OP: *De tabbladen 7, 8 en 9 zijn niet verplicht vanuit artikel 30 van de AVG, maar zijn wel een bruikbare aanvulling met betrekking tot autorisatie en daarom opgenomen in het dataregister.*



Als onderwijsinstelling wissel je niet alleen gegevens uit of laat je anderen in opdracht gegevens verwerken, maar ook intern worden er veel persoonsgegevens verwerkt. Dit tabblad is opgedeeld in interne gebruikers en interne applicaties.
Hoewel het aantal applicaties dat op eigen servers draait afneemt, is het wel van belang om te weten welke persoonsgegevens daarin worden vastgelegd.

Daarnaast worden veel gegevens opgeslagen in:

- leerling dossiers,
- inschrijfformulieren
- het ontwikkelperspectief (OPP)

Welke interne gebruikers hebben toegang nodig tot bepaalde persoonsgegevens en mogen die verwerken. Wat wil de instelling dat een docent kan zien aan persoonsgegevens, wat heeft hij/zij nodig om de werkzaamheden te doen. Dat geldt ook voor de afdeling PR, decanen en zorg-coördinatoren.
Geef bij IDM/ICT bijvoorbeeld aan welke gegevens de afdeling ICT kan zien (al dan niet in opdracht; zie tabblad 8 en 9) en welke gegevens nodig zijn om inloggegevens te genereren.
Dit tabblad kan gelijk als werkdocument gebruikt worden, eventueel aangepast met de benamingen die passen bij de eigen onderwijsinstelling.

5.5 Tabblad 8 en 9; Autorisaties

Tabblad 8 en 9 zijn een verdere uitwerking van 7. Tabblad 8 is toegespitst op de interne gebruiker. Hiermee kan de instelling een inventarisatie maken van de huidige toegang tot bepaalde categorieën van persoonsgegevens en wat volgens de AVG gewenst is. Hierbij moet rekening gehouden worden de met verwerkingsdoeleinden van de persoonsgegevens en grondslagen waarop een medewerkers, afdelingen die gegevens mogen verwerken. Tevens kan aangegeven worden tot welke organisatie onderdeel de medewerkers behoren en welke processen worden ondersteund.

Tabblad 8

		Interne gebruikers <schoolbestuur> XX>																	
			LAS / LVS																
		Medewerkers	erling administrat		Docent		Mentor		Decaan		Schoolleiding		IB-er / Zorg		PR		Afdeling ID		
		Organisatie onderdeel	organisatie breed		Toegewezen deel org.		Toegewezen deel org.		Toegewezen deel org		Toegewezen deel org		Intern		organisatie breed		eigen		
		Proces ondersteuning									Management informatie				Communicatie		Provisioning cy		
C: verwerkingsdoeleinden		Grondslagen																	
			Huidig	AVG	Huidig	AVG	Huidig	AVG	Huidig	AVG	Huidig	AVG	Huidig	AVG	Huidig	AVG	Huidig	AV	
	1a	Contactgegevens: naam, voornaam, e-mail en opleiding																	
		Naam																	
		Voornaam																	
		e-mail adres																	
		opleiding																	
	1b	Contactgegevens: geboortedatum en geslacht																	
		geslacht																	
		geboortedatum																	
	1c	Contactgegevens: overige gegevens																	
		adres																	
		postcode																	
		woonplaats																	
		telefoonnummer																	
		bankrekeningnummer																	
	2	Leerling nummer																	
	3	Nationaliteit en geboorteplaats																	
	4	Gegevens ouders/voogd																	
	5	Medische gegevens (vrijwillig / op eigen verzoek)																	
	6	Godsdienst (vrijwillig / op eigen verzoek)																	
	7	Studieverloop																	
		7a Examinering																	
		7b Traject voortgang																	
		7c Begeleiding Studenten																	
		7d Aanwezigheidsregistratie																	
		7e Medisch dossier (papier)																	
		7f Klas, leerjaar, opleiding																	
	8	Onderwijsorganisatie (roosters, beschikbaarheden, etc.)																	
	9	Financiën (volledige cyclus)																	
	10	Beeldmateriaal																	

Tabblad 9 is toegespitst op de interne applicaties en algemene documenten.
Tabblad 9

				Interne applicaties, documenten <schoolbestuur> XX>														
				Applicaties, documenten	Inschrijfformulier		Registratie incidenten		Medisch dossier						IDM		Netwerks	
				Organisatie onderdeel	Organisatie breed		Organisatie breed		Toegewezen deel org.		Toegewezen deel org		Toegewezen deel org		Organisatie breed		Organisatie	
C: verwerkings-doeleinden				Proces ondersteuning														
				Grondslagen														
					Huidig	AVG	Huidig	AVG	Huidig	AVG	Huidig	AVG	Huidig	AVG	Huidig	AVG	Huidig	
	1a	Contactgegevens: naam, voornaam, e-mail en opleiding																
			Naam															
			Voornaam															
			e-mail adres															
			opleiding															
	1b	Contactgegevens: geboortedatum en geslacht																
			geslacht															
			geboortedatum															
	1c	Contactgegevens: overige gegevens																
			adres															
			postcode															
			woonplaats															
			telefoonnummer															
			bankrekeningnummer															
	2	Leerling nummer																
	3	Nationaliteit en geboorteplaats																
	4	Gegevens ouders/voogd																
	5	Medische gegevens (vrijwillig / op eigen verzoek)																
	6	Godsdienst (vrijwillig / op eigen verzoek)																
	7	Studievoortgang																
			7a Examinering															
			7b Traject voortgang															
			7c Begeleiding Studenten															
			7d Aanwezigheidsregistratie															
			7e Medisch dossier (papier)															
			7f Klas, leerjaar, opleiding															
	8	Onderwijsorganisatie (roosters, boekenlijsten, etc.)																
	9	Financiën (volledige cyclus)																
	10	Beeldmateriaal																

5.6 Tabblad 10; Bewaartermijnen

		I Bewaartermijnen				
		Minimaal	Maximaal	Richtlijn	Start bewaartermijn	Wettelijke gron
I	(Digitaal) aanmeldingsformulier					
II	Kopie of inzage id/paspoort of DigID					
III	Document beheersmaatregel gezondheid					
IV	Overdrachtsformulier (o.a. OKR, OSO)					
V	Specifieke documenten*					
VI						
VII						
VII						
1a	Contactgegevens: geboortedatum en geslacht					
	naam					
	voornaam					
	e-mail adres					
	opleiding					
1b	Contactgegevens: geboortedatum en geslacht					
	geslacht					
	geboortedatum					
1c	Contactgegevens: overige gegevens					
	adres					
	postcode					
	woonplaats					
	telefoonnummer					
	bankrekeningnummer					
2	Leerlingnummer					

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 al ingevuld.
Bijlage 2 bevat een (concept)overzicht van de bewaartermijnen, die grotendeels is gebaseerd op de Wet bescherming persoonsgegeven.

Dit tabblad kan als werkdocument gebruikt worden om de bewaartermijnen vast te leggen.

LET OP: *Op dit moment wordt er gewerkt aan een overzicht van bewaartermijnen, waarin ook de archiefwet wordt opgenomen. Zodra deze beschikbaar is zal deze in de Aanpak IBP terug te vinden zijn.*

6 Het vullen van het dataregister

Het format dataregister voor leerlingen bestaat uit 1 document met verschillende voorbeeld werkdocumenten. In hoofdstuk 5 zijn deze werkdocumenten allemaal kort toegelicht en is de aanpasbaarheid en het gebruik ervan beschreven.
Maar waar ga je nu beginnen?
Sommige werkdocumenten moeten nu al ingevuld worden, andere werkdocumenten kunnen op een later moment. Deze gaan verder in op de details.
Dit hoofdstuk laat stap voor stap zien hoe het dataregister gevuld kan worden.

Logo Onderwijsinstelling

Register van de verwerkingsactiviteiten (Data register) Artikel 30 AVG

Dataregister 1

Versie: 16-2-2018

A	Contactgegevens van XX	Verwerkingsverantwoordelijke:	Vacature
		XX (voorzitter College van Bestuur)	Contactgegevens Functionaris Gegevensbescherm: ov@xx.nl
		Gemandateerd: XX (Bijvoorbeeld Directeur Bedrijfsvoering)	www.xx.nl

B	Categorie van de berokkene:	C	Verwerkingsdoeleinden:	Grondslag van de verwerkingsdoe	Doorgifte van persoonsgegevens buiten d
	Leerlingen PO/VO		a. Organiseren of het geven van onderwijs (w.o. onderwijsovereenkomst)	Wettelijk en overeenkomst	Niet van toepassing.
			b. berekenen, vastleggen en innen van 'gelden'	Overeenkomst, gerechtvaardigd belang	
			c. verantwoorden aan DUO, onderwijsinspectie en accountant	Wettelijke verplichting en overeenkomst	
			d. verstrekken van (digitale) leermiddelen	Overeenkomst, gerechtvaardigd belang	
			e. begeleiding leerling (pedagogisch dossier) en studieadvies	Wettelijk en overeenkomst	
			f. Onderzoek	Overeenkomst, gerechtvaardigd belang	
			g. uitvoering of toepassing van een andere wet of taak van algemeen belang	Wettelijk, overeenkomst, publ. taak	

J	Algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen	E	Brondocumenten	I	Bewaartermijnen	G	Gegevens van verwerkers (cloud)		
	voorbeeld: Assessment uitgevoerd op de informatiebeveiliging (ISO 27002), beoordeling volwassenheidsniveau 2,5 op basis van Toetsingskader SURF (schaal 1-5). Beoordeling uitgevoerd op Privacy (AVG2018), be-oordeling volgt.	I	(Digitaal) aanmeldingsformulier	2 jaar of 7 jaar (bekostiging)		naam	omschrijving	Website informatie (vb)	Datalocatie (vb)
		II	Kopie of inzage id/paspoort of DigID	Maximaal 1 maand	1	LAS / LVS: Magister	Studenten Informatie Systeem	www.magister.nl	Hengelo
		III	Doc. beheersmaatregel gezondheid	2 jaar of 7 jaar (bekostiging)	2	ELO:			
		IV	Overdrachtsformulier (o.a. OKR, OSO)	2 jaar n.b.o.	3	Toets:			
		V	Specifieke documenten**	2 of 7 jaar n.b.o.	4	Rooster:			
		VI			5	CRM:			
						Overig	Uitwerking overig en uitgeverijen in verwerkersoverzicht tabblad 5		

D	Categorieën van persoonsgegevens		F Andere verwerkingsverantwoordelijken									G Verwerkers						XX Interne gebruikers				Interne applicaties ****			BIV
			DUO	Leer plicht	school inspe	SWV	Accoun tant	GGD arts	CJP	Stage bedrijf	vervolg onderw	Overig ***	LAS 1	ELO 2	Toets 3	Rooster 4	CRM 5	Overig	leerling Admin.	docent	mentor	decaan	IB-er Zorg	PR overig	ICT IDM	Finan-cien	classificatie
1a	Contactgegevens: naam, e-mail, opleiding																										M-H-M
1b	Contactgegevens: geboortedatum en geslacht																										M-H-M
1c	Contactgegevens: overige gegevens																										M-H-M
2	Leerlingnummer																										M-H-M
3	Nationaliteit en geboorteplaats																										M-H-M
4	Gegevens ouders of voogd																										M-H-M
5	Medische gegevens (op eigen verzoek/vrijwillig)																										M-H-M
6	Godsdienst (op eigen verzoek/vrijwillig)																										M-H-M
7	Studie voortgang	7a Examinering																									M-H-M
		7b Studietraject																									M-M-M
		7c Begeleiding leerling																									M-M-M
		7d Aanwezigheidsregistratie																									M-H-M
		7e Medisch dossier (papier)																									M-H-H
		7f Klas, leerjaar, opleiding																									M-H-M
8	Onderwijsorganisatie (roosters, boekenlijsten, etc.)																										M-M-M
9	Financiën (volledige cyclus)																										M-H-M
10	Beeldmateriaal																										M-H-H
11	Docent/zorgcoördinator/ IB-er/ decaan/ mentor																										M-H-M
12	BSN (PGN)																										M-H-H
13	Eck-ID (keten ID)																										M-H-M
14	Overige gegevens																										M-H-M

Stap 1:

Begin met het invullen van de velden A, B en H. De opsomming van C (de verwerkingsdoeleinden) en grondslagen staan vast en de verwerkingsdoeleinden zijn al bij de categorieën persoonsgegevens ingevuld. Vul bij XX de naam van het schoolbestuur in.

LET OP: *De onderwijsinstelling blijft altijd zelf verantwoordelijk voor het juist invullen van de gegevens. Een ingevuld overzicht verandert hier niets aan.*

Stap 2:

Start met het inventariseren van de drie categorieën van verwerkers.

1. **Andere verwerkingsverantwoordelijken**; Het format heeft hiervoor al een aantal organisaties aangegeven. Te weten: *DUO, leerplicht, inspectie, samenwerkingsverband, accountant, GGD/schoolarts, cultureel jongeren paspoort (CJP), Stagebedrijven, vervolgonderwijs en overige waaronder Jeugdzorg/ wijkagent en diverse *logen.*
   Als er meerdere organisaties zijn die niet genoemd zijn dan kunnen die op tabblad 3 toegevoegd worden.

2. **Verwerkers;** Het format heeft ook hiervoor al een aantal opties aangegeven. Waaronder: *Leerling administratiesysteem/ leerling volgsysteem, elektronische leeromgeving (ELO), toetsing programma's, roosterprogramma, financiën, CRM.*
   En overige waaronder: studiebegeleiding, vastlegging/uitwisseling van zorg en overdracht gegevens, ouderportalen e.d. ten behoeve van communicatie, regionale samenwerkingsverbanden, bibliotheken, Cloud-omgevingen en de uitgeverijen /distributeurs.

   LET OP: *Bovengenoemde opties vallen alleen onder verwerkers als er in opdracht van de onderwijsinstelling gegevens worden verwerkt en uitgewisseld. Er worden dus persoonsgegevens elders opgeslagen. Applicaties en gegevens zijn online beschikbaar.*
   Met alle verwerkers moeten verwerkersovereenkomsten worden afgesloten, die voldoen aan de eisen van de AVG. Zie voor meer informatie: Aanpak IBP (http://kn.nu/ibponderwijs) en het privacyconvenant (https://www.privacyconvenant.nl/).

3. **Interne gebruikers (en applicaties);** Het format heeft ook hiervoor al een aantal opties aangegeven. Deze zijn te verdelen in *applicaties/algemene documenten binnen het eigen netwerk* en *medewerkers/afdelingen* die toegang hebben tot bepaalde persoonsgegevens (hier is een raakvlak met de autorisatiematrix, aangeven kan worden wie toegang heeft tot welke gegevens).
   Ook kan hier aangegeven worden welke gegevens worden vastgelegd in bijvoorbeeld het *inschrijfformulier, zorgdossier, of een registratieregister voor incidenten*.

   LET OP: *al deze gegevens worden verwerkt binnen de onderwijs*instelling *en dus opgeslagen op het eigen netwerk of gedeeld met eigen medewerkers.*

Voer alle geïnventariseerde onderdelen in het dataregister in.
- Gebruik voor verwerkingsverantwoordelijken tabblad 3
- Gebruik voor verwerkers tabblad 4, 5 en 6 zoals in hoofdstuk 5 beschreven.
- Gebruik voor interne gebruikers en applicaties tabblad 7, 8 en 9 zoals in hoofdstuk 5 beschreven.

Stap 3:
Nu moet er gekeken worden welke persoonsgegevens er waar verwerkt worden. Het advies is om dit samen te doen met de personen en of afdeling die er dagelijks mee te maken hebben. Zet vervolgens de vinkjes op de juiste plaatsen en laat het door een derde persoon controleren.

LET OP: *bij contactgegevens zijn er drie mogelijkheden; 1a, 1b en 1c. Deze komen op de tabbladen als een inklap reeks terug. Klik op het plusje in de kantlijn om de reeks open te vouwen en geef aan wat van toepassing is.*

Stap 4:
Gebruik het moment van vastleggen in het dataregister gelijk om een extra check te doen op de verwerkingsdoeleinden. Ga uit van het principe 'leg niet meer vast dan nodig is voor een bepaald doel'. Als er voor meer verwerkingsdoeleinden dan de 7 die onder C vermeld staan gegevens worden verzameld, leg dat dan vast en bepaal ook de grondslag op basis waarvan dit gebeurt.

Stap 5:
Vul de gegevens van de verwerkers G. in op tabblad 6 (de gegevens van de verwerkers). Geef de *omschrijving aan, de naam, website informatie, datalocatie* op bij het tabblad gegevens van verwerkers. Dit kan aangevuld worden met de afsluitdatum van de verwerkersovereenkomst en de versie.

De technische bijsluiter van de verwerkersovereenkomst kan gebruikt worden om naar te verwijzen bij genomen technische maatregelen. Voor communicatie met ouders/leerlingen kan verwezen worden naar de privacybijsluiter van de verwerkersovereenkomst (zie stap 7).

Stap 6:

Hou het dataregister up-to-date. Voer nieuwe verwerkingen direct in het register in, denk hierbij bijvoorbeeld aan nieuwe applicatie.
Regel processen in voor het aanschaffen van nieuw digitaal lesmateriaal, voor het afsluiten van nieuwe contracten of het aangaan van nieuwe samenwerkingen en/of uitwisselingen van gegevens.

LET OP:
Hiermee komt er een overlap met het uitvoeren van een Data Protection Impact Assessment (DPIA).
Een (D)PIA heeft de vorm van een toets-model of vragenlijst, met zowel feitelijke, technische als vragen over juridische eisen, waarmee organisaties voorafgaand aan een (nieuwe) gegevensverwerking de privacyrisico's voor de betrokkenen daarvan in kaart kunnen brengen. Vervolgens kunnen, indien nodig, maatregelen worden getroffen om de privacyrisico's te verkleinen.
Andersom geeft het dataregister ook input voor een eventueel uit te voeren (D)PIA.

> *Voorbeeld: bij het aanschaffen van een nieuw leerlingvolgsysteem, is vooraf al bekend welke gegevens worden vastgelegd in het huidige systeem en hoe de gegevens zijn geclassificeerd en beveiligd. Het nieuwe systeem zal dan ook minimaal aan deze eisen moeten voldoen.*

Stap 7:

Onderwijsinstellingen moeten leerlingen en/of ouders actief, laagdrempelig en in begrijpelijke taal informeren over hoe er met de persoonsgegevens van hun kind wordt omgegaan. Dit informeren moet op de volgende momenten:

- Als de school persoonsgegevens over leerlingen en/of ouders direct van hen verkrijgt, dan moet de school hen gelijktijdig (dus bij het verkrijgen van de gegevens) informeren over welke gegevens voor welk doel op basis van welke grondslag verwerkt worden en eventueel met wie deze gegevens verder worden gedeeld of niet gedeeld. Tevens moet vermeld worden hoelang de gegevens bewaard worden en wat de rechten van leerlingen en/of ouders zijn met betrekking tot hun gegevens. Ouders en/of leerlingen moeten ook weten welke gegevens zij verplicht zijn aan te leveren en wat de gevolgen zijn als zij deze gegevens niet geven.

- Daarnaast moet de onderwijsinstelling leerlingen en/of ouders op de hoogte brengen als persoonsgegevens indirect, dus via iemand anders, zijn verkregen. Hiervan moeten zij binnen één maand op de hoogte gebracht worden. Zie hiervoor *bijlage 4*

Het volgende hoofdstuk zal ingaan op het praktisch informeren van leerlingen en/of ouders over de gegevensverwerking. In een aantal gevallen hoeft de school leerlingen en/of ouders niet te informeren over de verwerking van de persoonsgegevens van hun kind.

7 Informeren van ouders (leerlingen) over de gegevensverwerking

Scholen verzamelen en gebruiken steeds meer persoonsgegevens van leerlingen (en ouders). Elke onderwijsinstelling is wettelijk verplicht om te verantwoorden wat er met die gegevens gedaan wordt. Ouders, en leerlingen (als zij 16 jaar en ouder zijn), hebben het recht om (ongevraagd) in begrijpelijke taal, uitgelegd te krijgen welke gegevens er van hun kind verwerkt worden en hoe privacy op school is geregeld. Zorg ervoor dat vragen over privacy beantwoord kunnen worden en er uitgelegd kan worden aan ouders (en leerlingen) wat de school doet met de persoonsgegevens van hun kind. Maak hierbij, indien van toepassing, onderscheid in de rechtstreeks van de ouders verkregen gegevens en de indirect verkregen gegevens, zoals beschreven in het vorige hoofdstuk.

Onderstaande toelichting kan gebruikt worden als informatie richting ouders over welke gegevens de school vastlegt van hun kind en hoe de privacy daarvan geregeld is.

7.1 Voorbeeld privacy toelichting omgaan met persoonsgegevens

Privacy toelichting ; Hoe gaat <Schoolbestuur> om met persoonsgegevens.

Contactgegevens <Schoolbestuur> :
Verwerkingsverantwoordelijke (bestuurder) van de school :
Contactgegevens Functionaris voor Gegevensbescherming :

<Schoolbestuur> verwerkt van al zijn leerlingen persoonsgegevens. <Schoolbestuur> vindt een goede omgang met persoonsgegevens van groot belang en is zich bewust van de privacywetgeving. <Schoolbestuur> is verantwoordelijk voor het zorgvuldig omgaan met de persoonsgegevens van uw kind. In deze privacy toelichting leggen wij u graag uit hoe wij met de persoonsgegevens van uw kind omgaan.

Waarom verwerken wij gegevens van uw kind
<Schoolbestuur> verwerkt persoonsgegevens van uw kind om onze verplichtingen als onderwijsinstelling te kunnen nakomen. Zo hebben wij bijvoorbeeld de gegevens nodig om uw kind aan te melden als leerling op onze school, om de studievoortgang bij te houden en om uw kind in staat te stellen een diploma te halen. Daarnaast hebben wij de wettelijke verplichting om bepaalde gegevens door te sturen naar andere partijen, zoals DUO (ministerie van Onderwijs) en leerplicht.
Wij verwerken gegevens van uw kind voor het uitvoeren van de *onderwijsovereenkomst* die we met uw kind hebben en/of voor het nakomen van onze *wettelijke verplichtingen.*
Gegevens die hier niet aan voldoen zullen wij alleen met uw toestemming verwerken. Als voor het verwerken van gegevens toestemming wordt gevraagd zoals voor het gebruik van beeldmateriaal (foto's en video's) dan kunt u de toestemming op elk moment intrekken of alsnog geven. (Wijziging van toestemming is niet van toepassing op inmiddels gepubliceerd beeldmateriaal).

Welke gegevens verwerken wij van uw kind
Wij verwerken diverse soorten gegevens, waarvan wij de meeste gegevens rechtstreeks van u als ouders hebben gekregen. U kunt hierbij denken aan contactgegevens en geboorteplaats. Als u weigert de voor ons noodzakelijke gegevens te verstrekken, kunnen wij onze verplichtingen niet nakomen. De verstrekking van deze gegevens is dan ook een voorwaarde om uw kind in te kunnen schrijven bij <schoolbestuur>.

Welke persoonsgegevens wij van uw kind verwerken kun u terugvinden onderaan deze toelichting bij Categorieën van persoonsgegevens.

Op uw eigen verzoek en met uw uitdrukkelijke toestemming verwerken wij ook medische gegevens van uw kind. Dit beperkt zich enkel tot gegevens die nodig zijn om in noodgevallen goed te kunnen handelen. U kunt bijvoorbeeld doorgeven dat uw kind epilepsie heeft, zodat wij adequaat kunnen optreden in noodsituaties. <Schoolbestuur> zal u nooit dwingen dergelijke gegevens te overleggen.

Hoe gaan wij om met de gegevens van uw kind
Bij het verwerken van de gegevens gaan wij altijd uit van noodzakelijkheid, wij zullen niet meer gegevens verwerken dan noodzakelijk is om onze rechten en plichten als onderwijsinstelling na te komen. Dit betekent ook dat de gegevens niet zullen gebruiken voor andere doeleinden dan wij in deze toelichting noemen.

In een aantal gevallen zijn wij, zoals eerder aangegeven, verplicht om gegevens van uw kind te delen met andere organisaties. Dit zijn onder andere DUO, leerplicht, de onderwijsinspectie, GGD/schoolarts, samenwerkingsverband en accountant.

Wij kunnen commerciële derde partijen verzoeken om te ondersteunen bij het verwerken van de gegevens voor de eerder genoemde doeleinden. Denk hierbij aan applicaties om leerlingen in de les te ondersteunen, een administratie systeem waarbij de gegevens niet op ons eigen netwerk worden opgeslagen, maar bij een andere organisatie of een lesroosterprogramma. Dit gebeurt altijd in opdracht en onder de verantwoordelijkheid van <schoolbestuur>. Met deze organisaties sluiten we overeenkomsten af, waarin o.a. is vastgelegd welke gegevens er verwerkt worden en hoe deze gegevens beveiligd worden.
Wij zullen de gegevens van uw kind niet delen met commerciële derde partijen voor andere doeleinden. Ook zullen wij de gegevens van uw kind nooit verkopen of verhuren aan derde partijen.

De persoonsgegevens worden zoveel mogelijk gecodeerd bewaard en alleen die medewerkers kunnen bij de gegevens, die dat ook voor de uitvoering van hun werk nodig hebben. Daarnaast bewaren wij de gegevens niet langer dan noodzakelijk is. Wij hanteren hiervoor verschillende bewaartermijnen die wettelijk geregeld en vastgesteld zijn. De bewaartermijn van gemaakte examens is bijvoorbeeld 2 jaar na het beëindigen van de onderwijsovereenkomst. Gegevens uit de leerling administratie worden over het algemeen 7 jaar bewaard. Als u er belangstelling voor heeft kunnen wij u een overzicht hiervan geven.

Welke rechten hebben een leerling en ouders van leerlingen jonger dan 16 jaar
Als ouders heeft u een aantal rechten als het gaat om persoonsgegevens. Deze rechten zijn in de wet vastgelegd. Leerlingen en/of ouders kunnen op elk moment gebruik maken van deze rechten. Dit betekent bijvoorbeeld dat u altijd een verzoek kunt indienen om inzage te krijgen in de gegevens die wij van uw kind verwerken.
Daarnaast kunt u ook een verzoek indienen om gegevens te rectificeren, te beperken of helemaal te wissen uit de systemen van <schoolbestuur>. U heeft altijd het recht om onjuiste gegevens aan te vullen of te verbeteren. Wij zullen er vervolgens voor zorgen dat deze gegevens ook bij organisaties waarmee wij deze gegevens van uw kind delen en/of uitwisselen worden aangepast.
Als u ons verzoekt om gegevens van uw kind te beperken of te wissen, zullen wij toetsen of dit mogelijk is. In deze toets houden wij ons aan de wettelijke voorschriften en kijken wij bijvoorbeeld of wij geen wettelijke plicht hebben om de gegevens te bewaren.
Tevens heeft u het recht om te vragen om de gegevens, die wij van uw kind verwerken en wij van u hebben ontvangen, aan u over te dragen of op uw verzoek aan een andere organisatie over te dragen. <Schoolbestuur> zal geen besluiten nemen over uw kind, die alleen gebaseerd zijn op geautomatiseerde verwerking van gegevens (profiling). Beslissingen worden nooit zonder menselijke tussenkomst genomen.

Als u het niet eens bent met hoe wij omgaan met de gegevens van uw kind, dan kunt u altijd opheldering vragen bij onze Functionaris voor Gegevensbescherming (zie de contactgegevens bovenaan deze toelichting). Indien uw probleem volgens u niet goed wordt opgelost, dan kunt u dat melden bij Autoriteit voor de Persoonsgegevens (www.autoriteitpersoonsgegevens.nl).

Opsomming van de categorieën van persoonsgegevens:

Categorie	Toelichting
1. Contactgegevens	**1a:** naam, voornaam, e-mail, opleiding *(bv. sector techniek)*; **1b:** geboortedatum, geslacht; **1c:** overige gegevens te weten: adres, postcode, woonplaats, telefoonnummer en eventueel andere voor communicatie benodigde gegevens, alsmede ook een bankrekeningnummer voor het afhandelen van betalingen**;**
2. Leerling nummer	een administratienummer dat geen andere informatie bevat dan bedoeld onder categorie 1
3. Nationaliteit en geboorteplaats	
4. Ouders, voogd	contact gegevens van de ouders/verzorgers van leerlingen (naam, voornaam, adres, postcode, woonplaats, telefoonnummer en eventueel e-mailadres)
5. Medische gegevens	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	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. Studievoortgang	gegevens betreffende de aard en het verloop van het onderwijs en de behaalde studieresultaten te weten: • Examinering (gegevens rondom het examen) • Studietraject • Begeleiding leerling (inclusief ontwikkelperspectief OPP) • Aanwezigheidsregistratie • Medisch dossier (papier) • Klas, leerjaar, opleiding
8. Onderwijsorganisatie	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. Financiën	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 /zorgcoördi-nator/ intern begeleider/ decaan / mentor	gegevens van **docenten en begeleiders,** voor zover deze gegevens van belang zijn voor de organisatie van de instelling en het geven van onderwijs, opleidingen en trainingen
12. BSN (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 contentketen'. Hiermee kunnen scholen gegevens delen, zonder dat ze direct herleidbaar zijn naar leerlingen of docenten.
14 Overige gegevens, te weten ….	andere dan de onder 1 tot en met 11 bedoelde gegevens waarvan de verwerking wordt vereist of noodzakelijk is met het oog op de toepassing van een andere wet. Deze zullen apart vermeld en toegelicht worden.

Bijlage 1: Grondslagen

Toelichting Grondslagen op basis van artikel 6 lid 1 AVG.

Grondslagen	Toelichting
A: 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
B: 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.
C: 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.
D: 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.
E: Publiekrechtelijke taak 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.
F: 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.

Bijlage 2: Bewaartermijnen

Uitgangspunt bij het omgaan met persoonsgegevens is dataminimalisatie. De verschillende soorten persoonsgegevens moeten redelijkerwijs nodig zijn om het doel te bereiken; ze moeten in verhouding staan tot het doel (proportioneel) en het doel kan niet met minder dan deze verzamelde gegevens worden bereikt (subsidiair). Het gaat er niet om dat er zo min mogelijk gegevens verzameld worden, maar om het verkrijgen van alleen díe gegevens die nodig zijn om het doel te bereiken. De vraag is hierbij hoe lang gegevens(sets) vervolgens mogen en/of moeten worden bewaard.
Een belangrijk onderscheid is de vraag, of het gegevens betreft die tot een persoon herleidbaar zijn. Als dat het geval is, dan is de privacywetgeving daarop van toepassing (tot 25 mei 2018 de Wbp, vanaf 25 mei 2018 de AVG).
Persoonsgegevens of set van gegevens moeten worden verwijderd wanneer deze niet meer nodig zijn. Voor het bewaren van persoonsgegevens(sets) zijn bewaartermijnen vastgelegd in de wet. Dit kan privacywetgeving zijn, maar ook andere wetgeving zoals het bekostigingsbesluit en examenbesluit . Het langer bewaren dan het voorgeschreven termijn is in strijd met de wet.

De Autoriteit Persoonsgegevens zegt over de bewaartermijnen onder de AVG het volgende:
"Zodra de Algemene verordening gegevensbescherming (AVG) van toepassing is, gelden dezelfde regels voor het bewaren van persoonsgegevens als nu. Het uitgangspunt blijft dat u persoonsgegevens niet langer mag bewaren dan noodzakelijk voor het doel van uw verwerking."

LET OP: Op dit moment wordt er gewerkt aan een totaaloverzicht van bewaartermijnen in samenspraak met OCW.

Enkele voorbeelden:

Document / gegevens	Wettelijke bewaartermijn	Ingangsdatum bewaartermijn
Gegevens over in– en uitschrijving	5 jaar	datum van uitschrijving
Gegevens over verzuim en afwezigheid	minimaal 5 jaar	datum van uitschrijving
Gegevens die nodig zijn om de bekostiging te berekenen	minimaal 7 jaar	na afloop van het schooljaar waarop de bekostiging betrekking heeft
Gegevens leerling na overstap naar speciaal onderwijs	3 jaar	datum van uitschrijving
Camera en videobeelden	maximaal 4 weken, dan wel na afhandeling van geconstateerde incidenten	moment van opname
Het onderwijskundig dossier	maximaal 2 jaar	datum van uitschrijving
Gezondheidgegevens die nodig zijn voor speciale begeleiding of voorzieningen	maximaal 2 jaar	datum van uitschrijving
Adresgegevens	maximaal 2 jaar	datum van uitschrijving
Werk centraal examen + cijferlijst	minimaal 6 maanden	na uitslag examen
Schoolexamens	maximaal 2 jaar	na uitslag examen

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.*

Bijlage 3: 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 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 4: 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.