



PRIVACY
OP SCHOOL

De AVG in het onderwijs *- wat u moet weten -*

Veelgestelde vragen uit het primair
en voortgezet onderwijs



www.privacyopschool.nl

Colofon

Uitgever en auteursrecht

Privacy op School
en Media Security Networks B.V.

www.privacyopschool.nl
www.yoursafetynet.com

Ondersteunend

Stichting BOOR, Rotterdam
Mr. Marleen Quaak en Drs. Ger Simjouw

Opmaak en ontwerp

QUEM Identiteit Makers, Dordrecht

Verkoopprijs: € 9,95

Alle rechten voorbehouden

Zonder voorafgaande schriftelijke toestemming van de uitgevers is het nadrukkelijk niet toegestaan deze uitgave:

Te vereenvoudigen, opslaan in een geautomatiseerd gegevensbestand, of openbaar maken, in enige vorm of enige wijze, hetzij elektronisch, mechanisch, door fotokopieën, opnamen of enige andere manier, zonder voorafgaande schriftelijke toestemming van de uitgevers.

Reprorecht

Voor zover het maken van kopieën uit deze uitgave is toegestaan op grond van artikel 16B Auteurswet 1912 jo het Besluit van 20 juni 1974, Stb. 351, zoals gewijzigd bij het Besluit van 23 augustus 1985, Stb. 471 en artikel 17 Auteurswet 1912, dient men de daarvoor wettelijk verschuldigde vergoedingen te voldoen aan Stichting Publicatie- en Reproductierechten Organisatie (PRO), Postbus 3060, 2130 KB Hoofddorp (www.cedar.nl/pro). Voor het overnemen van gedeelte(n) uit deze uitgave in bloemlezingen, readers en andere compilatiewerken (artikel 16 Auteurswet 1912) dient men zich tot de uitgever te wenden.

Bronvermelding

Voor zover het maken van kopieën uit deze uitgave door de uitgever zijn toegestaan dient altijd de bron conform het APA-format hierin te worden vermeld. De uitgever kiest ervoor zichzelf als werkgroep te identificeren. In dat geval dient de bronvermelding dit duidelijk te maken door de naam van de werkgroep zoals de publicatie vereist op de plek van de auteur te zetten:

- Bron: Werkgroep Privacy op School – YourSafetynet
- AVG/GDPR veelgestelde vragen: Onderwijs

Voorwoord

Sinds 25 mei 2018 is de Algemene Verordening Gegevensbescherming van toepassing in de Europese Unie, dus ook in Nederland. Ook in het onderwijs worden de effecten van deze wetgeving merkbaar en zichtbaar. Het onderwijs heeft nu eenmaal van doen met bijzondere persoonsgegevens en de verwerking daarvan. Gaandeweg de schoolloopbaan worden veel gegevens van leerlingen verzameld, opgeslagen en ook gedeeld. Het is van belang dat dit op een juiste manier gebeurt.

Privacy op School helpt scholen bij het concreet en behapbaar maken van de wetgeving in de onderwijspraktijk. Ondanks dat veel scholen en besturen op de goede weg zijn, is er nog een wereld te winnen. De nodige organisaties lopen vast in hun pogingen om de organisatie AVG-compliant te maken. Dat blijkt in de praktijk ingewikkeld en ingrijpend te zijn.

Los van het verwerken van gegevens binnen de organisatie hebben scholen ook te maken met partijen waarmee een verwerkersovereenkomst gesloten dient te worden.

Een van de oorzaken van het feit dat scholen het in de praktijk brengen van de AVG zo lastig vinden, ligt deels ook in de wetgeving zelf. Het juridisch jargon maken het voor mening persoon moeilijk te doorgronden.

Met het uitgeven van dit pocketformaat boekje willen we hier verandering in brengen. We versimpelen wat in basis ingewikkeld is en bieden praktische antwoorden op de meest belangrijke vragen.

Unieke samenwerking

De antwoorden op de vragen in dit boekje zijn tot stand gekomen dankzij de samenwerking tussen Privacy op School en YourSafetyNet.

Privacy op School heeft jarenlange ervaring in het onderwijs en weet alle ins en outs van het thema privacy. Onze adviseurs zijn op de hoogte van de laatste ontwikkelingen binnen het onderwijs én de AVG. Met onze tools, trainingen, ondersteuning en advies weet u zeker dat u uw informatiebeveiliging en privacy goed geregeld hebt. Samen met een team van enthousiaste juristen en adviseurs helpen we scholen om hun AVG-beleid vorm te geven.

YourSafetyNet is een plug-and-play softwaretool die de schoolorganisatie actief ondersteunt met de ontwikkeling, handhaving en controle van het AVG beleid en bestaat uit de AVG-wizard, AVG-workflow, AVG-boekhouding en AVG-zorgplicht.

Beide organisaties hebben hun sporen in het onderwijs verdiend en menig AVG-traject succesvol begeleid. Dankzij hun praktische en theoretische kennis op het gebied van gegevensbescherming zijn zij op een duidelijke manier, met klare taal in staat te antwoorden op kernvraagstukken.

Onze dank gaat daarnaast uit naar Stichting BOOR uit Rotterdam, die ons vanuit de praktijk van waardevolle input heeft voorzien.

Dit is een uitgave van:



Nadere kennismaking met Privacy op School

Graag bieden wij u de gelegenheid beter kennis te maken met Privacy op School. Hieronder benoemen we kort een aantal van onze belangrijkste producten en diensten.

Functionaris voor Gegevensbescherming

Elk schoolbestuur is verplicht een functionaris voor gegevensbescherming (FG) aan te wijzen. Deze taak mag ook extern belegd worden. Via Privacy op School kunt u een FG inhuren. Heeft u al een interne FG of wilt u eerst inzicht in hoe u ervoor staat? Dan kunnen wij voor u een (eenmalige) AVG audit uitvoeren. Met deze diensten ontlast u de druk in uw eigen organisatie en krijgt u inzicht in hoeverre u aan de privacywetgeving voldoet.

Opleiding en training

Onze tweedaagse opleiding is speciaal ontwikkeld voor PO en VO en geeft u alle tools in handen om invulling te geven aan uw positie als FG of IBP-functionaris binnen uw onderwijsomgeving. Daarnaast krijg u de gelegenheid een netwerk op te bouwen met andere privacy-professionals.

DPIA en risicoanalyse

Heeft uw school al inzichtelijk wat de grootste risico's zijn op het gebied van informatiebeveiliging en privacy? Wat zijn voor uw school passende maatregelen? Privacy op School voert regelmatig risicoanalyses uit voor onderwijsinstellingen.

Het uitvoeren van een DPIA is een tijdrovende klus. Privacy op School neemt u dit werk uit handen en legt de risico's bloot.

IBP-portaal

Het IBP-portaal is voorzien van content die aangepast wordt aan de laatste ontwikkelingen en waar u zo mee aan de slag kunt. Bovendien kunt u naar eigen wens gegevens toevoegen. Het platform bestaat uit drie onderdelen. Het portaal, bestaande uit een kennisbank, een IBP-dashboard en een online verwerkingsregister.

Bewustwording en voorlichting

Hoe gaan uw medewerkers om met privacygevoelige informatie? Zijn zij zich bewust van de risico's en gevolgen als er iets mis gaat? Onze AVG-voorlichtingsbijeenkomsten dragen bij aan het privacybewustzijn. Privacy op School verzorgt teamtrainingen en AVG-voorlichting waarin we de basisbeginselen van de AVG uitleggen. We vertellen wat een school moet regelen en wat daar een goede aanpak voor is.

E-learning

Wat is een datalek? Welke gegevens mag ik doorgeven aan een logopedist? Wat moet ik weten over filmen en fotograferen in het klaslokaal? Met onze betaalbare online cursus wordt de AVG met aansprekende voorbeelden vanuit de onderwijspraktijk uitgelegd. Al doende krijgt uw onderwijsprofessional kennis aangereikt op AVG-kwesties die zij in hun dagelijks werk tegenkomen. Onze e-learning biedt een module voor onderwijspersoneel en onderwijsondersteunend/overig personeel. Zo krijgt iedere medewerker alleen de relevante informatie voor zijn of haar functie.

Inhoud

Voorwoord	3
Nadere kennismaking met Privacy op School	5
Inhoud	7
Persoonsgegevens	8
Grondslagen	16
<i>Uitvoeren overeenkomst</i>	17
<i>Wettelijke plicht</i>	18
<i>Gerechtigd belang</i>	20
<i>Vitaal belang</i>	20
<i>Algemeen belang of uitoefening openbaar gezag</i>	21
<i>Toestemming</i>	22
Verwerkingsregister	27
Functionaris Gegevensbescherming	30
Verwerkersovereenkomst	33
Rechten van betrokkenen	36
Beveiligingsincidenten en datalekken	41
Overige vragen	45
Index	57

Persoonsgegevens

1. Wat zijn persoonsgegevens?

Sinds 25 mei 2018 is de Algemene Verordening Gegevensbescherming van toepassing binnen Nederland. De verordening reguleert de verwerking van persoonsgegevens in de hele Europese Unie en gaat vooral uit van het begrip *gegevensbescherming*.

Het onderwijs is bijzonder afhankelijk van persoonsgegevens. Sterker nog: het geven van onderwijs aan leerlingen zonder de verwerking van persoonsgegevens is geen optie. En wat te denken van alle administratie en HR-processen rondom medewerkers? Kortom, onderwijsorganisaties “lopen over” van persoonsgegevens.

Onder het begrip persoonsgegevens wordt verstaan: alle informatie over een natuurlijk persoon, een mens. Deze informatie gaat *direct* over iemand, of valt *indirect* naar iemand te herleiden. Wees er van bewust dat dit een bijzonder brede definitie is.

Voorbeeld:

Voor communicatie met de ouders verzamelt de leerkracht alle mailadressen van ouders. Nu, normaal gesproken, de meeste personen de eigen voor- en/of achternaam in het mailadres hebben staan, zijn mailadressen direct te herleiden naar personen. Daarom is een mailadres een persoonsgegeven.

Voorbeeld:

Voor het in kaart brengen van het voedingsgebied van de school verzamelt de administratie alle postcodes van alle leerlingen. Een postcode is niet direct naar een persoon te herleiden. Maar indirect kan een postcode, in combinatie met andere gegevens, toch naar een leerling te herleiden zijn. Er is hier dus toch sprake van een persoonsgegeven.

2. Wat is verwerking van persoonsgegevens?

De AVG is van toepassing wanneer er sprake is van *verwerking* van persoonsgegevens. Als er geen persoonsgegevens verwerkt worden is de AVG dan ook niet van toepassing. Verwerking gaat om alle handelingen die te maken hebben met persoonsgegevens. Verwerking is dus ook een breed begrip. Het kan dan bijvoorbeeld gaan om: verzamelen, vastleggen, ordenen, opslaan, bewerken, publiceren, opvragen en doorsturen van persoonsgegevens.

Soms wordt beweerd dat de AVG alleen van toepassing is op geautomatiseerde verwerking. Hierdoor zou de AVG lang niet altijd van toepassing zijn, omdat binnen het onderwijs een aantal administratieprocessen ook nog op papier worden uitgevoerd. De AVG is echter al heel snel van toepassing in het onderwijs. Zowel voor geautomatiseerde verwerking, gedeeltelijk geautomatiseerde verwerking én niet-geautomatiseerde verwerking, waarbij er sprake is van een bestand met persoonsgegevens, is de AVG van toepassing.

3. Wat zijn bijzondere persoonsgegevens?

Zoals eerder toegelicht is het begrip persoonsgegevens erg breed. Binnen het begrip persoonsgegevens bestaat de categorie “bijzondere persoonsgegevens”. Voor het verwerken van deze categorie persoonsgegevens bestaan extra regels. Deze gegevens zijn gevoelig en verdienen daardoor een hoger beveiligingsniveau. Wees ervan bewust dat het zeker niet onmogelijk is om gebruik te maken van bijzondere persoonsgegevens binnen schoolorganisaties. Om leerlingen onderwijs op maat aan te kunnen bieden zijn er eenmaal bijzondere persoonsgegevens nodig. Er moet dan wel sprake zijn van een gepaste uitzondering volgens artikel 9 AVG.

Bijzondere persoonsgegevens zijn gegevens over:

- Ras, etnische afkomst;
- Politieke opvattingen;
- Religieuze overtuigingen;
- Lidmaatschap van een vakbond;
- Genetische gegevens;
- Biometrische gegevens (zoals identificatiefoto's);
- Gezondheidsgegevens;
- Seksueel gedrag en seksuele gerichtheid.

Hoewel het BSN officieel gezien niet valt onder het begrip bijzondere persoonsgegevens, verdient de verwerking van het BSN toch extra aandacht en beveiliging. Voordat een BSN verwerkt wordt dienen er dus extra beveiligingsmaatregelen genomen te worden. Een nummer dat bij wet is voorgeschreven om een persoon te identificeren, mag alleen mag worden gebruikt voor de uitvoering van die wet. Of voor doeleinden die in de wet staan. Dat staat in artikel 87 van de AVG. Het BSN is zo'n identificatienummer.

Ook al geeft iemand toestemming om zijn BSN te gebruiken voor een andere grondslag dan genoemd in de AVG, betekent niet dat deze toestemming in alle gevallen geldig is. Kortom: toestemming doorbreekt niet het limitatieve wettelijk gekaderde gebruik van het BSN.

Voorbeeld:

Voor het inschrijven van leerlingen verzamelen scholen kopieën van ID-kaarten, waar het BSN op staat. Aangezien het BSN-nummer ook nodig is voor de inschrijving, kan deze niet afgeschermd of doorgekrast worden. De school heeft echter geen rechtmatige grondslag om na de inschrijving het BSN te bewaren. Een oplossing kan zijn door leerlingen ter plekke in te schrijven.

Of een wat praktischere oplossing: na het verwerken van de inschrijving, en het kopie-ID dus niet meer nodig is, de kopie onmiddellijk te vernietigen of terug te geven.

Verwerkt de school bijzondere persoonsgegevens? Het antwoord op deze vraag zal vaak met ja beantwoord kunnen worden. Kijk eerst of deze verwerking op grond van artikel 9 AVG is toegestaan. Neem daarna extra maatregelen.

4. Wat is een verwerkingsverantwoordelijke? Wat is een verwerker?

Zoals beschreven gaat het bij verwerking om alle handelingen die te maken hebben met persoonsgegevens. De AVG maakt onderscheid tussen twee actoren: de **verwerkingsverantwoordelijke** en de **verwerker**.

- De **verwerkingsverantwoordelijke** is degene die het *doel* en de *middelen* voor de verwerking van persoonsgegevens vaststelt.
- De **verwerker** is de partij die *ten behoeve van/in opdracht van* de verwerkingsverantwoordelijke persoonsgegevens verwerkt.

Het hangt dus af van de feitelijke situatie wie de verwerkingsverantwoordelijke is. Is de school degene die bepaalt welke persoonsgegevens worden verzameld, voor welk doel dit gebeurt en de manier waarop dit plaatsvindt (met welke middelen)? Dan is de school de verwerkingsverantwoordelijke. In de praktijk zal in veel gevallen een school dan ook te benoemen zijn als verwerkingsverantwoordelijke.

Voorbeeld:

Voor het aanbieden van digitaal lesmateriaal gebruikt een school digitale leermiddelen via een online portaal. Dit portaal is eigendom van de uitgeverij. Het portaal maakt gebruik van verschillende persoonsgegevens van leerlingen. Aangezien de school heeft bepaald hoe deze verwerking plaatsvindt en daarbij heeft gekozen voor betreffende uitgever, is de school de verwerkingsverantwoordelijke en de uitgever de verwerker.

Voorbeeld:

Een school kan veel persoonsgegevens doorzenden naar het samenwerkingsverband. Dit is vaak gebaseerd op een wettelijke plicht. Het samenwerkingsverband verwerkt de leerlinggegevens weer verder op de eigen manier en volgens de eigen taak. Zowel de school als het samenwerkingsverband zijn aan te merken als verwerkingsverantwoordelijke.

5. Wat zijn de beginselen van de AVG?

Iedere leerling, ouder of verzorger of medewerker (oftewel: de betrokkene) heeft het recht op bescherming van de persoonlijke levenssfeer. Dit is een grondrecht, ook privacy valt hieronder. Zo heeft iedere persoon het recht op privacy. Vanuit dit beginpunt zijn in de AVG zes beginselen geformuleerd, namelijk:

I. De verwerking van persoonsgegevens moet rechtmatig, behoorlijk en transparant zijn;

Handelen we als school behoorlijk en netjes? Heb ik de leerling of zijn ouders vooraf helder geïnformeerd over het doel van de gegevensverwerking? Heb ik uitgelegd welke gegevens worden gebruikt en met wie deze worden gedeeld?

II. De verwerking moet gebonden zijn aan specifieke verzameldoelen (“doelbinding”);

Heb ik vooraf een doel voor de verwerking van persoonsgegevens vastgesteld? Worden de persoonsgegevens alleen gebruikt voor dat doel dat ik vooraf heb vastgelegd?

III. De persoonsgegevens moeten toereikend zijn, ter zake dienend, en beperkt tot wat noodzakelijk is (“minimale gegevensverwerking”);

Gebruik ik alleen die gegevens die noodzakelijk zijn om het vastgestelde doel te verwezenlijken? Kan ik met minder of bijvoorbeeld anonieme gegevens werken? Bewaar ik de gegevens niet langer dan nodig?

IV. De gegevens moeten juist zijn (“juistheid”);

Kloppen de persoonsgegevens die ik gebruik nog steeds? Verwijder ik persoonsgegevens als school actief wanneer gegevens onjuist of verouderd zijn?

V. De gegevens mogen niet langer worden bewaard dan nodig (“opslagbeperking”);

Bestaan er binnen de school bewaartermijnen? Worden deze bewaartermijnen in praktijk ook nageleefd?

VI. Gegevens moeten goed beveiligd zijn en vertrouwelijk blijven (“integriteit en vertrouwelijkheid”).

Zijn de gegevens op het juiste moment, op de juiste plaats en voor de juiste mensen beschikbaar? Heb ik onjuiste gegevens gecorrigeerd of verwijderd? Voldoe ik aan de datalekmeldplicht wanneer deze van toepassing is?

Grondslagen

6. Wat is een grondslag?

Iedere verwerking moet gebaseerd zijn op een in de AVG genoemde grondslag. Zonder grondslag is de verwerking niet rechtmatig en dus wettelijk niet toegestaan. Er moet minimaal één grondslag aanwezig zijn. Het bepalen van de grondslag moet vooraf gebeuren. Dit kan dus niet achteraf, of pas wanneer ouders of leerlingen om duidelijkheid vragen.

Is er geen grondslag? Dan mogen de gegevens **niet** verwerkt worden.

7. Moeten de grondslagen vastgelegd worden?

Ja. De onderwijsinstelling heeft een verantwoordingsplicht. Dat betekent dat de instelling moet kunnen aantonen dat de verwerkingen aan de regels van de AVG voldoen. Om dit te kunnen aantonen moet dit ergens worden vastgelegd, bijvoorbeeld in het verwerkingsregister.

8. Wat zijn de grondslagen?

Er mag alleen verwerking van persoonsgegevens plaatsvinden wanneer:

- Dit nodig is voor het *uitvoeren van een (onderwijs)overeenkomst*;
- Er een *wettelijke plicht* bestaat om deze gegevens te verstrekken;

- Er sprake is van een *gerechtvaardigd belang*;
- Er sprake is van een *vitaal belang*;
- Wanneer dit *noodzakelijk is voor een taak in het algemeen belang of voor de uitoefening van het openbaar gezag*;
- Er *toestemming* is verkregen.

Bovenstaande grondslagen worden hierna nader uitgewerkt.

Twijfels over de toepasselijke grondslag? Laat je dan altijd adviseren. Het hanteren van de onjuiste grondslag kan ernstige gevolgen hebben.

9. Ik verwerk als particulier persoonsgegevens voor persoonlijk gebruik. Is dat toegestaan?

Ja, u mag als individu in de privésfeer persoonsgegevens verwerken. Denk bijvoorbeeld aan het voeren van een verjaardagskalender of een persoonlijk adresboek. De regels voor de AVG gelden in dat geval niet. Maar let op: wanneer er al in enige mate sprake is van een zakelijke activiteit, is de AVG al van toepassing.

Uitvoeren overeenkomst

10. Wanneer is er sprake van het uitvoeren van een overeenkomst?

De school heeft de primaire verplichting het onderwijs te verzorgen voor de leerlingen. Alle leerprocessen en gegevensverwerkingen die betrekking hebben op het bieden van dit onderwijs kunnen op deze grondslag gebaseerd worden. Dit kan bijvoorbeeld gaan om het verzamelen van persoonsgegevens voor de inschrijving of de verwerking van persoonsgegevens binnen het LVS-systeem.

Wettelijke plicht

11. Wanneer is er sprake van een wettelijke verplichting?

Wanneer de gegevensverwerking noodzakelijk is voor het nakomen van een wettelijke verplichting, is er ook sprake van een rechtmatige grondslag. Een voorbeeld: de verwerking van persoonsgegevens met betrekking tot de overdracht PO naar VO is wettelijk geregeld. De school hoeft dus geen toestemming aan de ouders te vragen, maar mag bepaalde dossiers en informatie overdragen naar de nieuwe school.

12. Mag de leerplichtambtenaar persoonsgegevens ontvangen?

Leerplichtambtenaren voeren een wettelijke taak uit en hebben het recht op bepaalde informatie. Op basis van de grondslag wettelijke plicht mogen er dus gegevens aan de leerplichtambtenaar verschaft worden. Daarbij gaat het vooral om gegevens met betrekking tot verzuim. Let wel op het beginsel van de dataminimalisatie.

Sommige gemeenten hanteren een zogenaamde 'preventieve aanpak'. Dit kan echter op gespannen voet staan met de AVG, omdat er soms wel signalen zijn dat ongeoorloofd verzuim wordt verwacht, maar er feitelijk nog niet is. In dat geval mogen geen persoonsgegevens worden gedeeld met de leerplichtambtenaar.

13. Mag de Inspectie van het Onderwijs toegang krijgen tot persoonsgegevens?

De Inspectie van het Onderwijs mag op grond van een wettelijke taak toegang krijgen tot persoonsgegevens.

14. Mag de school gegevens verstrekken aan Veilig Thuis¹?

Op grond van de Wet maatschappelijke ondersteuning en de Uitvoeringswet AVG heeft Veilig Thuis de wettelijke plicht om gegevens over gezondheid en gegevens over kindermishandeling en huiselijk geweld te verwerken. Ter bescherming van het kind mogen scholen in bepaalde gevallen daarom persoonsgegevens verstrekken aan Veilig Thuis.

Ga voor meer informatie naar www.veiligthuis.nl

¹ *Kindermishandeling komt in Nederland meer dan 119.000 keer per jaar voor. Dat betekent dat gemiddeld in iedere schoolklas van 30 leerlingen 1 kind zit dat wordt mishandeld. Kindermishandeling kan fysiek of psychisch geweld zijn, maar ook verwaarlozing. Bijvoorbeeld ouders die schreeuwen tegen hun kind of vaak negatieve dingen zeggen. Vaak doen ouders dit omdat ze niet goed weten hoe ze met hun kinderen om moeten gaan. Dit noemen we opvoedonmacht. Maar soms zijn kinderen op een andere manier slachtoffer. Bijvoorbeeld als ze slachtoffer zijn van seksueel misbruik, of getuige zijn van huiselijk geweld.*

Bron: <https://veiligthuis.nl/huiselijk-geweld-en-mishandeling/>

15. Kunnen persoonsgegevens op grond van een wettelijke plicht worden doorgegeven aan de vervolgschool?

Verhuist een leerling (PO naar PO, VO naar VO), of verlaat een leerling de basisschool (PO naar VO) dan mogen op grond van de Wet PO en de Wet VO persoonsgegevens worden doorgegeven aan de vervolgschool.

Gerechtvaardigd belang

16. Wanneer is er sprake van een gerechtvaardigd belang?

Het verwerken van persoonsgegevens wat gebaseerd is op de grondslag gerechtvaardigd belang kan soms lastig zijn. Het gerechtvaardigd belang is namelijk een rekbare norm. Een voorbeeld van een gerechtvaardigd belang binnen het onderwijs kan zijn: het verwerken van medewerkersgegevens van de onderwijsorganisatie voor managementrapportages. Wil je een verwerking baseren op de grondslag gerechtvaardigd belang? Dan is het aan te raden om extern advies te vragen, hiervoor een motivatie te laten opstellen en deze memo op te nemen in je AVG-boekhouding.

Vitaal belang

17. Wanneer is er sprake van de bescherming van vitale belangen?

Wanneer het echt noodzakelijk is om de vitale belangen van iemand te beschermen, kan een verwerking gebaseerd worden op de grondslag vitaal belang. Dit moet gaan om levensbedreigende situaties waarbij het noodzakelijk is dat, bijvoorbeeld, de school bepaalde gegevens acuut aan hulpverleners moet doorgeven. Het verwerken van persoonsgegevens op basis van deze grondslag is alleen toegestaan indien het niet op basis van een andere grondslag kan worden gebaseerd. Vaak zal het nog mogelijk zijn om jezelf te beroepen op de grondslag toestemming.

Algemeen belang of uitoefening openbaar gezag

18. Wanneer is er sprake van de grondslag *algemeen belang of de uitoefening van het openbaar gezag?*

Het gaat hierbij vaak om wettelijk vastgestelde taken. De verwerking moet in dat geval een grondslag hebben in het recht van de Europese Unie of dat van een lidstaat, ook het doeleinde van de verwerking moet hierin beschreven zijn. Voor scholen is deze grondslag verder niet relevant.

Toestemming

19. Hoe houd ik het vragen van toestemming werkbaar?

Sinds 25 mei 2018 – de inwerkingtreding van de AVG – hebben scholen er een forse administratieve last bijgekregen: toestemmingsformulieren. Tenminste, zo kan het lijken. Onterecht is de indruk ontstaan dat nu voor ieder “wissewasje” expliciete toestemming nodig is. Sommige scholen maken daarom gebruik van bijzonder uitgebreide toestemmingsformulieren. Dat is niet per se noodzakelijk!

Het is niet nodig om bij inschrijving van de leerling toestemming te vragen voor vermelding van geslaagden in de krant en op de website. Veel gemakkelijker is het om dit tijdens het examenjaar te regelen, bijvoorbeeld door de mentor. Vanwege de examenvoorbereidingen is de kans tot het krijgen van toestemming mogelijk groter.

Indien de school incidenteel een tweet op Twitter plaatst, is het niet nodig om aan alle leerlingen toestemming te vragen voor publicatie van foto's. Het is veel efficiënter om de leerlingen, of ouders, om toestemming te vragen op het moment dat er echt een bericht met foto geplaatst wordt.

Veel oudercommunicatieportalen zijn inmiddels ook AVG-proof. Het portaal zelf regelt en registreert toestemming voor de school. In dat geval is het niet nodig om via een formulier nogmaals toestemming te vragen voor het delen van oudercommunicatiegegevens. Vermijd het vragen van dubbele toestemming, dat kost tijd. Tijd is schaars, zeker in het onderwijs.

Heel basaal gezegd kan toestemming op twee manieren geregeld worden binnen een school. Ten eerste kan toestemming gevraagd worden via een formulier dat is verstrekt aan alle leerlingen of ouders. Voor bepaalde schoolactiviteiten is dat nou eenmaal nodig, bijvoorbeeld de schoolfoto's. Het is ook mogelijk om toestemming pas te vragen wanneer het echt nodig is, ter plekke of vooraf. Toestemming nodig voor een foto van een select groepje leerlingen bij een bepaalde activiteit? Probeer mondelinge toestemming te vermijden, omdat dit achteraf niet te verifiëren is.

Kortom; het is goed het toestemmingsbeleid eens tegen het licht te houden. Sla niet door en vraag geen onnodige toestemming op onnodige momenten. Houd het werkbaar.

20. Zijn er wettelijke eisen voor het vragen van toestemming?

Rechtsgeldige toestemming moet voldoen aan de volgende eisen:

- de toestemming moet *vrijelijk gegeven* worden;
- de gegeven toestemming moet *ondubbelzinnig* zijn;
- de persoon die toestemming geeft moet voldoende worden *geïnformeerd*;
- de toestemming moet *specifiek* zijn.

21. Moet toestemming schriftelijk worden gegeven?

Toestemming moet je kunnen aantonen. Houd een administratie of register bij van de gegeven toestemming. Dit is dé reden dat mondelinge toestemming – soms heel praktisch - wordt afgeraden: mondeling gegeven toestemming is lastig te bewijzen. Zorg dus dat je de toestemmingsverklaringen schriftelijk of digitaal organiseert, zodat er een toestemmingsadministratie bijgehouden kan worden.

22. Is toestemming nodig voor het gebruik van foto's?

De hoofdregel is: wanneer een school foto's gebruikt heeft deze altijd toestemming nodig voor het gebruik van foto's.

23. Is toestemming nodig voor het doorgeven van persoonsgegevens aan de vervolgopleiding?

Voor het doorgeven van gegevens van PO naar VO scholen is geen toestemming nodig. Hiervoor bestaat namelijk een wettelijke grondslag.

Voor het doorgeven van gegevens aan MBO scholen is wel toestemming nodig. Voor de gegevensuitwisseling VO-MBO is geen wettelijke plicht, waardoor er ook geen wettelijke grondslag bestaat. De ouder of leerling moet dus expliciet toestemming geven voor de uitwisseling van leer(begeleiding)gegevens tussen de VO en MBO school.

24. Hoe vraag ik om toestemming?

Het wordt aangeraden om de toestemmingsvraag schriftelijk te organiseren. In het geval van steeds terugkomend foto- en videomateriaal, van een sportdag, schoolkamp, etc., is het bovendien raadzaam om de toestemming al bij de inschrijving van de leerling of indiensttreding van een werknemer te regelen.

25. Wanneer vraag je toestemming?

In verschillende situaties kan het nodig zijn om toestemming aan de ouders te vragen, namelijk als er geen andere AVG-grondslag voorhanden is. Bijvoorbeeld als je persoonsgegevens deelt met externe deskundigen zoals logopedisten, RT'ers, psychologen etc. Maar ook als je persoonsgegevens deelt doordat je leerlingen opdraagt een sociale media-account (zoals Pinterest) te laten aanmaken om te gebruiken in de les.

26. Moet ik ieder jaar opnieuw toestemming vragen

voor het verwerken van persoonsgegevens?

Zoals eerder vermeld is dit niet noodzakelijk. Wel is het belangrijk om een eenmaal gegeven toestemming, bijvoorbeeld voor foto- en videogebruik van leerlingen, jaarlijks onder de aandacht te brengen. Daarbij moet de betrokkene er ook op gewezen worden dat hij zijn toestemming alsnog kan wijzigen of intrekken. Ouders kunnen hun toestemming bijvoorbeeld zodanig wijzigen dat foto's van hun kind niet langer op de website van school gepubliceerd mag worden, maar nog wel in de schoolgids.

27. Vanaf welke leeftijd moet een leerling onder de AVG zelf toestemming geven voor het verwerken van zijn/haar persoonsgegevens?

Vanaf 16 jaar. Van leerlingen jonger dan 16 jaar is toestemming dus alleen geldig wanneer deze door een van de ouders is gegeven.

28. Aan wie moet ik toestemming vragen als de ouders zijn gescheiden?

Bij kinderen onder de 16 jaar moet je toestemming vragen aan degene die het ouderlijk gezag toekomt. Dit is niet altijd een ouder, maar kan ook een voogd zijn. In de regel hebben beide ouders echter gezamenlijk het ouderlijk gezag. Een scheiding verandert daar in principe niets aan. Als het ouderlijk gezag aan beide ouders gezamenlijk toekomt, mag je toch afgaan op de toestemming of weigering van één van de ouders. Ouders moeten namelijk zelf aan de school kenbaar maken als zij er samen niet uitkomen. Als je signalen krijgt dat de ouders het onderling niet eens zijn over de toestemming, moet je de verwerking stopzetten totdat de ouders weer op één lijn zitten.

29. Maakt het uit of foto's of filmpjes gepubliceerd

worden of alleen worden opgeslagen?

Nee. De vraag is niet of er iets gepubliceerd wordt, maar of er persoonsgegevens verwerkt worden. Opslaan valt ook onder verwerken.

30. Hoe zit het wanneer ouders foto's en filmpjes publiceren op sociale media?

Zo ver gaat de verantwoordelijkheid van de school niet. Vraag als school of de ouders terughoudend willen zijn met het maken van foto's en video's binnen de school en deze foto's niet te delen via sociale media.

Verwerkingsregister

31. Wat is het register voor de gegevensverwerkingen?

De AVG dient *aantoonbaar* nageleefd te worden. Alle verwerkingsactiviteiten moeten dus ergens te worden bijgehouden en geregistreerd. De school heeft daarom een plicht tot het maken en bijhouden van een verwerkingsregister. In dit register staat een opsomming van onder andere, alle verwerkingen, doeleinden, categorieën van de betrokkenen en de ontvangers, bewaartermijnen en een beschrijving van technische en organisatorische beveiligingsmaatregelen, locatie van deze opslag, etc.

32. Is een verwerkingsregister verplicht?

Niet iedere organisatie is verplicht een verwerkingsregister bij te houden. Aangezien er op scholen structureel bijzondere persoonsgegevens worden verwerkt, is een register wel een wettelijke verplichting. Bij een eventuele controle van de Autoriteit Persoonsgegevens zal een register vaak als eerste uitgevraagd worden: het geeft immers een structureel overzicht van alle verwerkingsactiviteiten.

33. Wat heeft een onderwijsorganisatie aan een verwerkingsregister?

Naast alle bestaande lasten en administratieve handelingen hebben scholen en schoolbesturen er door de AVG een verplichting bij: het opstellen van een register van verwerkingsactiviteiten, oftewel een verwerkingsregister. Een flink document waar veel werkuren in zitten: inventariseren, overleggen, uitwerken en structureren.

Toch is het creëren van een verwerkingsregister niet alleen een wettelijke plicht of een “verplicht nummertje”, het is juist een kans voor jouw onderwijsorganisatie!

Het opstellen van een verwerkingsregister:

- biedt inzicht in de organisatiestructuur;
- identificeert onrechtmatige verwerkingen en verkeerde bewaarplaatsen;
- laat een organisatie nadenken over bewaartermijnen;
- creëert een fundament voor de organisatie, FG en AP;
- kan duidelijkheid geven bij incidenten;
- geeft een actueel up-to-date document omtrent verwerkingen persoonsgegevens.

Functionaris Gegevensbescherming

34. Wat is een Functionaris voor Gegevensbescherming?

De eerste door de wetgever bedeelde rol aan de Functionaris Gegevensbescherming is het houden van toezicht. Dit toezichthouden is tweeledig: de Functionaris dient zowel toe te zien op de naleving van wettelijke verplichtingen vanuit de AVG, als op de naleving van het interne IBP-beleid. De Functionaris monitort en ziet toe op de privacy compliancy van de school. De Functionaris moet, naast het houden van toezicht, de school uitgebreid kunnen adviseren en informeren.

De Functionaris Gegevensbescherming is als toezichthouder hét contactpunt voor de AP. De Functionaris is er niet alleen voor de organisatie en het bestuur, deze persoon dient immers ook toe te zien op de gegevensbescherming van leerlingen, ouders en medewerkers. En uiteraard ingrijpen (rapporteren en waarschuwen) mocht de school zich niet houden aan de AVG.

35. Is het aanstellen van een Functionaris verplicht?

Het aanstellen van een Functionaris Gegevensbescherming is lang niet in alle gevallen verplicht. Zo heeft niet ieder Nederlands bedrijf of instelling deze verplichting. Scholen hebben deze verplichting **wel** wegens het stelselmatig observeren van leerlingen (bijv. LVS en OPP's) en op grote schaal verwerken van bijzondere persoonsgegevens.

36. Kan er gebruik gemaakt worden van een externe FG?

De Functionaris moet goed op de hoogte zijn van de Europese en nationale privacywetgeving en van de praktijk van gegevensbescherming. Dit betekent in ieder geval dat de Functionaris voldoende inzicht moet hebben in de gegevensverwerkingen van de school, kennis en ervaring moet hebben van ICT en informatiebeveiliging. Daarnaast moet de Functionaris inzicht hebben in de informatiesystemen die de school gebruikt en de behoeften van de school op het gebied van veiligheid van gegevens en gegevensbescherming. De Functionaris moet een onafhankelijke positie in de school hebben. Om de onafhankelijke rol van de Functionaris te waarborgen is dit juist een argument om van een externe Functionaris gebruik te maken.

37. Waar moet ik de Functionaris Gegevensbescherming aanmelden?

De Functionaris moet dient te worden aangemeld bij de Autoriteit Persoonsgegevens, via een online formulier op de website van de Autoriteit Persoonsgegevens: <https://autoriteitpersoonsgegevens.nl>

Verwerkers- overeenkomst

38. Wat is een verwerkersovereenkomst?

De verwerker en de verwerkingsverantwoordelijke dienen bepaalde afspraken vast te leggen. Hierin worden zaken als de aansprakelijkheid, bewaartermijnen, rechten en verplichtingen en alle informatie omtrent de verwerking vastgelegd. De wet verplicht zowel de verwerkingsverantwoordelijke en de verwerker om tot deze overeenkomst te komen.

39. Wat is het Privacy Convenant?

Het Convenant Digitale Onderwijsmiddelen en Privacy vertaalt de AVG naar de onderwijspraktijk. Het bevat afspraken over het omgaan met persoonsgegevens bij het gebruik van digitale leermiddelen en toetsen. Dankzij het convenant weten scholen en aanbieders wat ze over en weer van elkaar mogen verwachten, zijn de afspraken werkbaar in de praktijk en heeft iedereen dezelfde gemeenschappelijke uitleg bij deze afspraken.

Alle aangesloten deelnemers maken gebruik van eenzelfde model verwerkersovereenkomst. Hierdoor is de opbouw hetzelfde, al kan de inhoud wel verschillen.

40. Wiens verantwoordelijkheid is het om een overeenkomst af te sluiten?

De AVG verplicht zowel de verwerkingsverantwoordelijke als de verwerker om gezamenlijk tot deze overeenkomst te komen.

41. Waar moet ik op letten bij een verwerkersovereenkomst?

Het verdient de voorkeur om verwerkersovereenkomsten te laten beoordelen door een jurist en/of (externe) deskundige. Dat kan nare (aansprakelijkheids)gevolgen voorkomen. Een aantal tips waar de school zelf, voorafgaand aan de beoordeling, naar kan kijken:

- Bekijk of er wordt voldaan aan de eisen van art. 28 AVG;
- Wanneer een verwerkersovereenkomst in de vorm van een convenant van toepassing is:
 - › Wordt dit convenant in zijn geheel, zonder verwijderingen, toevoegingen of beperkingen gebruikt?
 - › Indien één of meerdere artikelen uit dit convenant niet van toepassing zijn, wordt dit dan in de verwerkersovereenkomst nadrukkelijk vermeld met motivatie van waarom?
- Wordt de huidige wetgeving benoemd (AVG), i.p.v. de verouderde wetgeving (WBP)?
- Let op de aansprakelijkheidsregeling;
- Heeft verwerker een deugdelijke aansprakelijkheidsverzekering afgesloten die ook het risico van cyberincidenten dekt?
- Voldoet verwerker onvoorwaardelijk aan de thans geldende AVG?
- Let op onduidelijke termen en termijnen in de overeenkomst.

Rechten van betrokkenen

42. Wat zijn de rechten van betrokkenen?

De AVG geeft, logischerwijs, betrokkenen rechten met betrekking tot hun persoonsgegevens. Door deze rechten kunnen ouders, leerlingen en medewerkers opkomen voor hun privacy. Verzoeken kunnen niet door de school genegeerd worden, de rechten van betrokkenen zijn wettelijk vastgelegd. Als organisatie moet je niet alleen aan allerlei technische en organisatorische eisen voldoen, maar ook aan verzoeken gehoor kunnen geven. De school heeft de verplichting om te voldoen aan deze verzoeken.

Het gaat om het:

- recht op dataportabiliteit;
- recht op vergetelheid;
- recht op inzage;
- recht op rectificatie en aanvulling;
- recht op beperking van de verwerking;
- recht om bezwaar te maken.

43. Wat is het recht op dataportabiliteit?

Op grond van de AVG kunnen betrokkenen persoonsgegevens opvragen om ze vervolgens naar een andere organisatie of instelling over te dragen. Dit recht is nauw verwant met het recht op inzage.

44. Wat is het recht op vergetelheid?

Vergetelheid staat voor het wissen van gegevens. Dit recht houdt dan ook in dat een onderwijsinstelling in bepaalde gevallen iemands persoonsgegevens moet wissen indien hiervoor een verzoek ontvangen is. Niet alle gegevens kunnen en mogen altijd gewist worden. Zo heeft een school wettelijke verplichting tot het bewaren van bepaalde gegevens.

45. Moeten gegevens alleen verwijderd worden na een verzoek m.b.t. het recht van vergetelheid?

Nee. Gegevens moeten sowieso actief verwijderd worden wanneer de organisatie de gegevens zelf niet meer nodig heeft, de bewaartermijn verlopen is, de toestemming is ingetrokken of een andere grondslag is vervallen.

46. Wat is het recht op inzage?

Betrokkenen hebben het inzagerecht tot alle persoonsgegevens die over de betrokkene zelf verwerkt worden. Ouders en leerlingen hebben dus het inzagerecht tot alle gegevens die over de leerling verwerkt worden. Medewerkers hebben het inzagerecht tot alle gegevens die over de medewerker zelf vastgelegd zijn.

47. Mag een ouder inzage tot alle gegevens, of mag de inzage worden beperkt tot het LAS/LVS?

Ouders hebben het recht om alle persoonsgegevens van hun kind die door de school worden verwerkt in te zien. De inzage mag dus niet worden beperkt.

48. Wat is het recht op rectificatie en aanvulling?

Betrokkenen kunnen vragen foutieve gegevens te rectificeren en eventueel verder aan te vullen. Het gaat dus om foutieve gegevens, ouders hebben niet het recht om alle gegevens te laten rectificeren waar ze niet mee eens zijn.

49. Welke termijnen gelden er voor het reageren op de in te roepen rechten?

In principe dient een verzoek zo snel mogelijk te worden afgehandeld. De wet spreekt zelf van “onverwijd”, wat zoiets betekent als: zonder uitstel. Sommige verzoeken zullen toch wat tijd nodig hebben. In ieder geval geldt de termijn van één maand.

Is er sprake van een complex verzoek, of een groot aantal verzoeken van dezelfde betrokkene? Dan is het mogelijk om een verlenging van twee maanden te hanteren. Deze verlenging moet wel onderbouwd worden. Verlenging of niet, in ieder geval dient er een reactie na één maand verzonden te worden.

50. Gelden deze rechten ook voor mijn medewerkers?

Ja. Wanneer de AVG spreekt over betrokkenen is dit een breed begrip. Dit kunnen zowel leerlingen, ouders, leveranciers, huurders en juist ook medewerkers zijn. Een werkgever verwerkt een grote set aan persoonsgegevens van medewerkers. Ook medewerkers hebben daarom bovengenoemde privacyrechten. Zorg en ontwikkel dan ook samen met je P&O of HR-afdeling procedures die betrekking hebben op deze in te roepen rechten. Uiteraard dient de MR hierbij als deelgenoot betrokken te worden.

51. Waar kan ik de procedures vinden ten aanzien van de uitvoering AVG-zorgplicht?

Neem hiervoor contact op met de Privacy Officer of de Functionaris Gegevensbescherming van jouw organisatie. Wanneer de organisatie gebruik maakt van tooling zoals bijvoorbeeld YourSafetynet of het IBP-portaal van Privacy op School, dan is deze informatie daarin terug te vinden.

Beveiligingsincidenten en datalekken

52. Wat is een datalek?

Op een school kunnen verschillende beveiligingsincidenten plaatsvinden. Wanneer er bij deze beveiligingsincidenten persoonsgegevens betrokken zijn is er al snel sprake van een datalek. Een datalek is *een inbreuk op de beveiliging en bescherming van persoonsgegevens die ook leidt tot een ongeoorloofde verwerking van persoonsgegevens*. Dit is een brede definitie. Ook per ongeluk of onrechtmatige vernietiging van persoonsgegevens kan vallen onder een datalek.

53. Wanneer moet een datalek vastgelegd worden?

Elk voorgevallen datalek dient intern geregistreerd te worden. Organisaties dienen daarom een datalekregister bij te houden. Hier worden alle belangrijke zaken rondom het datalek vermeld (feiten, gevolgen en corrigerende maatregelen). Dit register is handig voor de organisatie, maar dient ook als overzicht die de Autoriteit Persoonsgegevens kan opvragen in het geval van een controle.

54. Wanneer moet een datalek gemeld worden aan de Autoriteit Persoonsgegevens?

De hoofdregel is dat een datalek gemeld moet worden bij de Autoriteit Persoonsgegevens.

Hierop bestaat een uitzondering, die in praktijk van toepassing kan zijn. Wanneer het onwaarschijnlijk is dat de inbreuk gevolgen en een risico voor de betrokkenen veroorzaakt hoeft het datalek niet gemeld te worden (maar dus wel intern gedocumenteerd!).

Moet het datalek gemeld worden? Dan dient dit binnen 72 uur te gebeuren. Deze termijn gaat in nadat de verwerkingsverantwoordelijke van het (mogelijke) datalek kennis heeft genomen.

55. Is er sprake van een datalek wanneer er niemand toegang heeft verkregen?

Het kan voorkomen dat bepaalde informatie publiekelijk online te bereiken is, bijvoorbeeld door het veranderen of wijzigen van een URL. Kan de school geheel uitsluiten dat er iemand toegang heeft verkregen tot deze persoonsgegevens? Dan is er geen sprake van een datalek. Zijn er geen logs bijgehouden, of kan er niet uitgesloten worden dat een onbevoegde toegang heeft verkregen? Dan dient dit wel gezien te worden als een datalek.

56. Wanneer moet een datalek gemeld worden aan de betrokkene(n)?

Heeft zich een datalek voorgedaan? Dan moeten in bepaalde gevallen de betrokkenen (bijvoorbeeld leerlingen of ouders) geïnformeerd worden, het gaat immers om een incident met betrekking tot persoonsgegevens van die betrokkene *zelf*. Er dient een melding te gaan naar betrokkenen wanneer de inbreuk een *hoog risico* inhoudt voor de rechten en vrijheden van natuurlijke personen. De term *hoog risico* is een wat vage norm. In ieder geval is er sprake van een hoog risico wanneer de betrokkenen negatieve gevolgen zal ervaren door het datalek

57. Waar kan ik de procedures vinden ten aanzien van melding beveiligingsincident?

Neem hiervoor contact op met de Privacy Officer of De Functionaris Gegevensbescherming van jouw organisatie. Wanneer de organisatie gebruik maakt van tooling zoals bijvoorbeeld YourSafetynet of het IBP-portaal van Privacy op School, dan is deze informatie daarin terug te vinden.

Overige vragen

58. **Waarom hoeft de pers geen toestemming te vragen?**

Om de journalistiek niet te beperken en de vrijheid van meningsuiting niet onder de voeten te lopen is in de AVG een journalistieke exceptie opgenomen. Deze uitzondering regelt dat bepaalde delen van de AVG dan niet van toepassing zijn. Scholen kunnen zich soms op deze uitzondering beroepen.

59. **Hoe ga ik om met situaties waarin iets moet vanuit de AVG, terwijl het technisch of praktisch niet uitvoerbaar is?**

In een geval waarin je niet volgens de AVG kunt handelen, probeer je zoveel mogelijk in de **geest** van de AVG te handelen. Dit doe je door de beginselen uit de AVG zo goed mogelijk toe te passen op de situatie. Het uitgangspunt is altijd: Voorkom ten alle tijden het onrechtmatig verwerken van persoonsgegevens wat nadelige gevolgen kan hebben voor de betrokkenen.

60. Hoe voldoe ik aan de informatieplicht?

De school moet ouders en leerlingen informeren over de persoonsgegevens die de school verwerkt. Dit was onder de vorige wetgeving ook al het geval. Leerlingen en ouders moeten namelijk weten welke gegevens je over hen verzamelt en wat je er mee doet. De manier om aan de informatieplicht te voldoen, is door het aanbieden van een privacyverklaring.

61. Wat is een privacyverklaring?

Om in zijn algemeenheid aan de informatieplicht te voldoen stelt de school een privacyverklaring op en publiceert deze op de website. In de verklaring staan alle verwerkingen, doeleinden, grondslagen en andere wettelijk vereiste informatie samengevat. Het is belangrijk dat de school geen informatie achterhoudt. Wees dan ook volledig transparant in de verklaring. Zorg dat de privacyverklaring voor het publiek te begrijpen is (voor zowel leerlingen en ouders). Vermijd zoveel mogelijk complex juridisch taalgebruik.

62. Geldt de informatieplicht ook voor mijn medewerkers?

Ja. Wanneer de AVG spreekt over betrokkenen is dit een breed begrip. Dit kunnen zowel leerlingen, ouders, leveranciers, huurders en juist ook medewerkers zijn. Een werkgever verwerkt een grote set aan persoonsgegevens van medewerkers. Ook medewerkers hebben daarom het recht op informatie met betrekking tot hun privacy. Stel daarom een interne privacyverklaring op, of breid de huidige privacyverklaring uit met een gedeelte over de verwerking van medewerkersgegevens. Ook sollicitanten hebben het recht om te weten wat er met hun persoonsgegevens gebeurt.

63. Is de bewustwording van medewerkers een optie of een wettelijke verplichting?

Volgens de AVG dienen organisatorische maatregelen getroffen te worden. De organisatie dient dus privacy compliant te zijn. Daar valt ook bewustwording, voorlichting en eventuele verdere opleiding van het personeel onder. Bewustwording van medewerkers kan dus zeker gezien worden als een wettelijke verplichting. Met de e-learningmodule van Privacy op School kunt u aantoonbaar maken dat uw medewerker beschikt over de basiskennis AVG.

64. Mogen ouders nog toegang tot leerlinggegevens na het 16e levensjaar?

Vanaf 16 jaar hebben leerlingen zelfstandige privacyrechten. Dit betekent echter niet dat ouders geen toegang meer mogen hebben tot studievoortgangsgegevens of het LVS. In de Wet op het Voortgezet Onderwijs is namelijk geregeld dat een school verplicht is om de ouders van 16- en 17-jarige leerlingen te informeren over de vorderingen van de leerling. Hiervoor hoeft dus geen toestemming te worden gevraagd. Let op: toestemming is wel nodig wanneer een leerling 18 jaar is geworden. De leerling is dan immers geheel zelfstandig, meerderjarig en handelingsbekwaam.

65. Mag je nog CC mailen?

De AVG verbiedt CC mailen niet. De AVG verbiedt het ongevraagd, zonder grondslag, delen van persoonsgegevens wel. Aangezien de meeste mailadressen bestaan uit persoonsnamen, dient gelijktijdig CC mailen naar meerdere personen of groepen vermeden te worden.

66. Mogen leerlingendossiers en/of medische gegevens nog op USB-sticks gezet worden?

Pas op met het uitwisselen van bestanden op onbeveiligde wijze. Dossiers bevatten vaak zoveel bijzondere persoonsgegevens, dat de gevolgen na een beveiligingsincident zo groot kunnen zijn dat er extra maatregelen genomen dienen te worden. Bestanden met deze gevoelige waarde dienen dan ook beveiligd te worden.

Datadragers als usb-sticks, dvd's, laptops, tablets en harde schijven kunnen kwijtraken en zo datalekken veroorzaken. Voorzie datadragers daarom, om misbruik van de 'verloren' data te voorkomen, van encryptie (dataversleuteling) in combinatie met een wachtwoord. Sommige USB-sticks, laptops en tablets zijn hier al standaard mee uitgevoerd. Voor datadragers die niet voorzien zijn van encryptie software in combinatie met een wachtwoord kan gebruik gemaakt worden van encryptiesoftware.

67. Mogen we in ons onderwijs onze leerlingen gebruik laten maken van sociale media?

Voor bepaalde digitale onderwijsmiddelen moeten leerlingen soms gebruik maken van sociale media, denk aan het uploaden van een filmpje op YouTube. Hiervoor moeten leerlingen een account aanmaken, in opdracht van de school. Er vloeien dan persoonsgegevens van de school naar het sociale mediabedrijf. De belangrijke vraag is dan: is er een rechtmatige grondslag? Voor veel digitale lesmiddelen kan de grondslag gebaseerd worden op het uitvoeren van overeenkomst of het gerechtvaardigd belang. Voor het aanmaken van sociale media-accounts is dit lastig: deze accounts zijn immers veel breder te gebruiken dan alleen als onderwijsmiddel. Hiervoor dient dan ook toestemming aan de ouders gevraagd te worden wanneer er geen andere grondslag voorhanden is.

68. Onze externe netwerkbeheerder heeft zichzelf toestemming gegeven tot alle mailboxen, mag dat?

Met de netwerkbeheerder is waarschijnlijk een verwerkersovereenkomst (met geheimhoudingsverklaring) afgesloten. Het schoolbestuur blijft namelijk verantwoordelijk voor deze verwerking van persoonsgegevens (e-mails kunnen inzien van werknemers). Deze vraag ligt daarmee op de grens van privacyrecht en arbeidsrecht. Vanwege het privé karakter van de mails van een medewerker en het recht op privacy, mag de werkgever zich slechts in uitzonderlijke gevallen toegang verschaffen tot de mailbox van een medewerker.

Namelijk als:

- de medewerker op de hoogte is of zou kunnen zijn dat de mail gecontroleerd kan worden;
- de werkgever een gerechtvaardigd belang heeft om mails te controleren; en
- er is voldaan aan de proportionaliteitseis (de inbreuk op de privacy moet in verhouding staan tot het belang van de werkgever).

De netwerkbeheertaken zouden een gerechtvaardigd belang kunnen vormen voor het schoolbestuur om in geval van een incident in de inbox van een medewerker te kunnen (mee)kijken. Van deze mogelijkheid moet het personeel vooraf dus wel op de hoogte zijn. Verder moet naar de netwerkbeheerder toe duidelijk zijn dat zij in beginsel geen e-mails mogen inzien. De werkgever zou de netwerkbeheerder hierop kunnen controleren. Dit soort afspraken moeten ook uitgebreid in de **verwerkersovereenkomst** worden opgenomen.

69. Wat is privacy by design en privacy by default?

In het kader van de AVG wordt vaak gesproken over privacy by design en privacy by default. Deze begrippen zijn zeer relevant voor onderwijsorganisaties en de gecontracteerde ICT-leveranciers.

Privacy by design: De wet spreekt van gegevensbescherming door ontwerp. Voordat een systeem of proces in gebruik wordt genomen dient al rekening gehouden te worden met de beginselen van gegevensbescherming.

Privacy by default: De wet spreekt van gegevensbescherming door standaardinstellingen. Gegevensbescherming is zo belangrijk waardoor software en systemen altijd privacy-vriendelijk moeten worden ingesteld.

70. Heeft de AVG gevolgen voor autorisaties?

Ja. Op basis van privacy by design dient er bij de (her)inrichting van systemen gebruik gemaakt te worden van autorisaties. Niet iedere medewerker dient tot dezelfde set persoonsgegevens toegang te hebben. Op basis hiervan is het wenselijk om gebruik te maken van autorisaties. Om deze autorisaties te verantwoorden kan een autorisatiematrix worden opgesteld.

71. Is logging met betrekking tot systeemtoegang en autorisaties verplicht?

Het opstellen van autorisatiematrixen heeft alleen betrekking op processen. Deze processen dienen dan ook in praktijk toegepast te worden. Leidinggevenden hebben hierin samen met de ICT-afdeling een belangrijke taak. Beveiligingsmaatregelen dienen niet alleen beleidsmatig vastgelegd, maar ook gecontroleerd te worden. Het periodiek controleren van de logs wordt dan ook dringend geadviseerd. Uiteraard dient dit protocol wel bij medewerkers bekend te zijn.

72. Over welke documenten dient de school nog meer te beschikken?

Al eerder werd het gebruik van een privacyverklaring, toestemmingsformulieren, verwerkingsregister en datalekregister aangeraden. Dat is nog niet alles, het is ook wenselijk om de volgende documenten op te stellen:

- Procedure voor datalekken, in het kader van bewustwording onder medewerkers;
- Protocollen en gedragsregels voor medewerkers, in het kader van afspraken met medewerkers, bijvoorbeeld over het gebruik van geleende devices;
- Protocollen en gedragsregels voor leerlingen, in het kader van bewustwording van leerlingen bijvoorbeeld door het gebruik van sociale media;
- Geheimhoudingsverklaringen, voor interne of externe medewerkers die te maken krijgen met privacygevoelige data;
- Beleid rondom het gebruik van cameratoezicht, in het kader van zowel de verantwoordings- als informatieplicht.

73. Is een schoolmaatschappelijk werker (SMW'er) een verwerkingsverantwoordelijke, verwerker of onderdeel van de school?

Het hangt er helemaal vanaf hoe de relatie tussen school en SMW in elkaar zit. Een SMW'er kan in dienst zijn van de gemeentelijke jeugdzorg), een zorgorganisatie, het samenwerkingsverband of de school zelf.

Bepaalt de school het doel en de middelen van de verwerking? Dit zal, in ieder geval, zo zijn wanneer de SMW'er in dienst is, of ingehuurd wordt, door de school. In andere gevallen zal de organisatie waar de SMW'er onder valt vaak de verwerkingsverantwoordelijke zijn, zoals het CJG.

74. Wat is een DPIA?

Wanneer een verwerking van persoonsgegevens waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen, dan moet de schoolorganisatie een gegevensbeschermingseffectbeoordeling (DPIA) uitvoeren. Zo'n DPIA moet in principe voorafgaand aan de invoering van de verwerking plaatsvinden. Echter, in het kader van de implementatie van de AVG moeten schoolorganisaties ook alle huidige processen die een hoog risico kunnen inhouden voor de rechten en vrijheden van natuurlijke personen door middel van een DPIA beoordelen.

Een DPIA onderzoekt en beoordeelt de effecten van een nieuwe verwerking. Te denken valt aan een project m.b.t. medische gegevens, het gebruik van beveiligingscamera's, een nieuw HR-systeem of nieuwe LVS-software. Een DPIA brengt verhoogde beveiligingsrisico's in kaart, die scholen vervolgens op basis van deze rapportage kunnen minimaliseren.

75. Wat is de rol van een Functionaris Gegevensbescherming bij een DPIA?

Aangezien de rol van de Functionaris toezichthoudend en adviserend is, dient de Functionaris advies uit te brengen bij het uitvoeren van de DPIA. Dit advies dient verwerkt te worden in de DPIA. De Functionaris hoeft niet de persoon te zijn die de DPIA uitvoert.

76. Wanneer is een DPIA sowieso verplicht?

De Autoriteit Persoonsgegevens heeft een lijst samengesteld van verwerkingen waarbij een DPIA in ieder geval uitgevoerd dient te worden. Deze lijst is dus niet-limitatief!

Een DPIA dient in ieder geval uitgevoerd te worden
wanneer er sprake is van:

- Heimelijk onderzoek
- Zwarte lijsten
- Fraudebestrijding
- Creditscores
- Financiële situaties
- Genetische persoonsgegevens
- Gezondheidsgegevens
- Samenwerkingsverbanden
- Cameratoezicht
- Controle werknemers
- Locatiegegevens
- Communicatiegegevens
- Internet of Things
- Profiling
- Biometrische gegevens
- Monitoring en beïnvloeding van gedrag

Bron: www.autoriteitpersoonsgegevens.nl

Met name het profiling (van leerprestaties of gezondheid), het monitoren en beïnvloeden van gedrag, het verwerken van communicatiegegevens, cameratoezicht en de controle van werknemers zullen van toepassing zijn binnen een schoolorganisatie. Voor deze processen dient dan vaak een DPIA uitgevoerd te worden.

77. Hoe lang mag je e-mails bewaren in je mailbox?

De inhoud van e-mails kan zo verschillen dat er geen standaard bewaartermijn van e-mails bestaat. Het gaat om de categorie persoonsgegevens in de mail zelf. Een mailbox is alleen maar een communicatiemiddel, de e-mail zelf of de bijlage is aan te merken als de verwerking. Zorg dus dat er binnen de school een vastgesteld bewaartermijnenbeleid bestaat. En dat bewustwording bij de medewerkers onder de aandacht wordt gebracht, waardoor ook de persoonlijke mailboxen van medewerkers periodiek worden geschoond.

78. Wat zijn de geldende bewaartermijnen in het onderwijs?

In de AVG zijn geen bewaartermijnen beschreven. Deze dienen door de school zelf te worden vastgesteld. De hoofdregel is dat persoonsgegevens niet langer worden bewaard dan noodzakelijk is voor de verwerking, of zo lang noodzakelijk is op grond van een wettelijke verplichting.

Veel leerling(dossier)gegevens kunnen tot twee jaar na datum van uitschrijving worden bewaard. Gegevens met betrekking tot de bekostiging van de school kunnen tot zeven jaar worden bewaard na de datum van uitschrijving. Data over de in- en uitschrijving en het verzuim van de leerling kunnen tot 5 jaar bewaard worden vanaf de datum van uitschrijving.

Met betrekking tot medewerkersgegevens kunnen de meeste gegevens bewaard worden tot twee jaar na uitdiensttreding. Gegevens omtrent loonadministratie, burgerlijke staat en andere fiscaal relevante gegevens kunnen tot 7 jaar bewaard worden na uitdiensttreding.

Kijk ook eens op: <https://aanpakibp.kennisnet.nl/>

79. Mogen namen van medewerkers gecommuniceerd worden via de schoolgids?

Ook medewerkers hebben het recht op de bescherming van hun privacy. Betekent dit dat de schoolgids ook geen personeelsnamen meer mag bevatten? De schoolgids heeft als doel het informeren van ouders en andere betrokkenen rondom schoolactiviteiten en de schoolorganisatie. Hiervoor kan het noodzakelijk zijn om medewerkersnamen te communiceren. Zo is het voor ouders relevant om te weten wat de naam is van een leerkracht of mentor. Indien dit noodzakelijk is, is het vermelden van personeelsnamen in de schoolgids toegestaan. Hiervoor is geen toestemming nodig van de desbetreffende medewerker.

80. Het is handiger om het leerlingvolgsysteem in zijn geheel open te stellen voor alle medewerkers, is dat toegestaan?

Medewerkers mogen alleen toegang hebben tot persoonsgegevens *die zij voor de uitvoering van hun taken nodig hebben*. Het kan dus in geen geval zo zijn dat iedere leraar toegang heeft tot alle leerlinggegevens. Maak gebruik van het autorisatiesysteem wat binnen het LVS beschikbaar is.

Degene die binnen de school of het bestuur verantwoordelijk is voor de autorisatie (vaak de bovenschools ict-coördinator) kan hierin een belangrijke rol vervullen.

Index

	Vraag	AVG-artikel
Autorisaties	70-71, 80	24, 25
Beginselen	5	5
Bewaartermijnen	77-78	5
Bewustwording	63	
Burgerservicenummer	3	46 Uitv. wet
Datalek	52-57	33, 34
Datalekregister	53	33
Documentenbibliotheek	72	
Doelbinding	5	5
Doelmatigheid	5	5
DPIA	74	
Functionaris voor Gegevensbescherming	34-37	37-39
Gerechtigd belang	8, 16	6
Grondslag	6	6
Informatieplicht	60-62	12-14, 19, 21
Integriteit	5	5
Juistheid	5	5
Leeftijdsgrens	27, 64	5 Uitv. wet
Minimale gegevensverwerking	5	5
Opslagbeperking	5	5

	Vraag	AVG-artikel
Pers en journalistiek	58	6
Persoonsgegevens	1	4, 9, 10
Persoonsgegevens, bijzonder	3	9
Privacy by default	69	24, 25
Privacy by design	69	24, 25
Privacy Convenant	39	
Privacyverklaring	61-62	12-14
Publiekrechtelijke taak	7, 16	6
Recht op dataportabiliteit	43	20
Recht op inzage	46-47	15, 20
Recht op rectificatie en aanvulling	48	16
Recht op vergetelheid	44-45	17
Rechten van betrokkenen	42-51	12-23
Rechten van betrokkenen, termijnen	49	12
Rechtmatigheid	5	5
Register van de verwerkingen	31-33	30
Toegangsbeveiliging	70-71	24, 25
Toestemming	7, 19-30	4, 6-9
Transparantie	5	5
Uitvoering overeenkomst	7, 8	6
Verantwoordingsplicht	6	5
Verwerker	4	4
Verwerkersovereenkomst	38-41	28
Verwerking	2	4, 5, 6
Verwerkingsregister	31-33	30
Verwerkingsverantwoordelijke	4	4
Vitaal belang	8, 15	6
Wettelijke plicht	8, 11-15	6



PRIVACY
OP SCHOOL

Privacy op School

Ga voor meer informatie en downloads naar:

www.privacyopschool.nl