



# 2

Katern

Wegwijzer

Wet bescherming persoonsgegevens

vos ) a b b



## Wet bescherming persoonsgegevens

vos ) a b b

Bezoekadres: Polanerbaan 15, Woerden

Postadres: Postbus 162, 3440 AD Woerden

Telefoon: 0348 - 40 52 00

Fax: 0348 - 40 52 05

E-mail: [secretariaatvereniging@vosabb.nl](mailto:secretariaatvereniging@vosabb.nl)

Website: [www.vosabb.nl](http://www.vosabb.nl)



## Inhoud

Inleiding	4
1. Wet- en regelgeving	5
2. College Bescherming Persoonsgegevens	7
3. Intern toezicht op verwerking van gegevens	7
4. Verwerking van gegevens in schoolpraktijk	8
5. Verwerking van gegevens voor leerlingenadministratie	12
6. Foto's, video-opnamen, webcam en internet	15
7. E-mail	16
8. Computerapparatuur	18
9. Zorg- en adviesteam	18
10. Gegevensverwerking van zieke werknemer	19
11. Persoonsgebonden nummer bij uitwisseling leerling- en begeleidingsgegevens	21
12. Sociale media	22
13. Tot besluit	23



## Inleiding

Privacybescherming is in dit digitale tijdperk actueler dan ooit. Waar gegevens worden verwerkt, rijzen voortdurend vragen. Dat is ook zo in het onderwijs. Hoe moet u handelen als de gemeente gegevens van leerlingen opvraagt voor het Gemeentelijk Onderwijs Achterstandenbeleid? Moet u bij een echtscheiding beide ouders informeren over de resultaten van hun kind? Kan een werknemer gegevens uit zijn personeelsdossier laten verwijderen? En kunt u klassenfoto's zonder problemen op de website van uw school plaatsen?

Deze online herziening van het katern uit 2006 gaat in op dergelijke vragen en biedt daarbij een aantal handreikingen voor de schoolpraktijk. Ook wordt ingegaan op de hoofdlijnen van wet- en regelgeving over privacybescherming. De herziening is alleen digitaal en uit kostenoverwegingen niet in druk uitgebracht.

VOS/ABB, september 2013



## 1 Wet- en regelgeving

De Wet bescherming persoonsgegevens (WBP)<sup>1</sup> beoogt ieders recht op privacy te waarborgen, onder meer door eisen te stellen aan de verwerking van persoonsgegevens. Hieronder wordt verstaan elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens. Voorbeelden zijn het verzamelen, vastleggen, bijwerken, raadplegen en doorgeven van gegevens.

Volgens de wet zijn persoonsgegevens alle gegevens die iets over een persoon zeggen of die van invloed kunnen zijn op de manier waarop een persoon wordt beoordeeld of behandeld. Hieronder wordt onder andere begrepen de naam, geboortedatum en adres van betrokkene, maar ook zijn bankrekeningnummer en het kenteken van zijn auto. De gegevens moeten tot de persoon herleidbaar zijn. De wet bestrijkt dus een ruim terrein. Zo valt ook het registreren van beelden en het maken van geluidsopnamen van personen onder de reikwijdte van deze wet.

Behalve de wetstekst geldt het Vrijstellingsbesluit bescherming persoonsgegevens. In dit besluit worden uitzonderingen van wettelijke bepalingen geregeld en bijzondere regels gegeven voor bepaalde beroepsgroepen.

### Wettelijke uitgangspunten

De wet stelt de privacybescherming voorop bij de belangen van organisaties en instanties die persoonsgegevens verwerken. Deze gegevens mogen derhalve slechts worden verwerkt als de persoon hiervoor ondubbelzinnig (dat wil zeggen: schriftelijk) voorafgaande toestemming heeft verleend en de verwerking ervan in overeenstemming geschiedt met een wettelijk toegestaan doel. De verwerking van persoonsgegevens moet volgens de wet worden gemeld bij het College Bescherming Persoonsgegevens (CBP), tenzij hiervoor vrijstelling bestaat of is verleend.

Verwerking van zogenoemde bijzondere persoonsgegevens is in beginsel verboden. Het gaat hierbij om gegevens zoals:

- godsdienst/levensovertuiging;
- ras;
- politieke gezindheid;
- gezondheid;
- seksueel leven;
- lidmaatschap vakvereniging;
- strafrechtelijke gegevens e.d.

Als echter sprake is van uitvoering van wetten of

---

<sup>1</sup> In werking getreden op 1 september 2001

overeenkomsten, kunnen hierop uitzonderingen worden gemaakt. De WBP geeft aan wie onder welke voorwaarden bijzondere gegevens mag verwerken. Het verbod geldt ook niet als sprake is van uitdrukkelijke toestemming van de betrokkene.

### **Voorbeelden**

Het verwerken van gegevens over de gezondheid van leerlingen is wel toegestaan als dit bijvoorbeeld geschiedt met het oog op het kunnen begeleiden van leerlingen of het treffen van bijzondere voorzieningen in verband met hun gezondheid. Als een personeelslid ziek is, kan de arbodienst de verkregen gegevens administratief verwerken voor de ziekteverzuimbegeleiding. Een ziek personeelslid hoeft overigens zijn werkgever niet mee te delen wat hem of haar mankeert. In hoofdstuk 10 wordt de gegevensverwerking bij een zieke werknemer nader uitgewerkt.

### **Vrijstellingsbesluit**

Naast de WBP geldt het Vrijstellingsbesluit Wet bescherming persoonsgegevens (hierna te noemen: het Vrijstellingsbesluit). In beginsel dienen persoonsregistraties en het verwerken van persoonsgegevens te worden gemeld aan het CBP. In dit uitvoeringsbesluit worden enkele veelvoorkomende verwerkingen van persoonsgegevens vrijgesteld van deze meldings-

plicht. De bepalingen in het Vrijstellingsbesluit moeten hierbij wel in acht worden genomen. Ze ontslaan de verwerker niet van de plicht om eventueel andere zaken wel bij het CBP te melden als hierover niets in het Vrijstellingsbesluit is geregeld. De bepalingen van het Vrijstellingsbesluit staan op [www.cbpweb.nl](http://www.cbpweb.nl) en [www.wetten.nl](http://www.wetten.nl).



## 2 College Bescherming Persoonsgegevens

Voor een goede uitvoering van de WBP is een toezichthoudend orgaan ingesteld: het College Bescherming Persoonsgegevens (CBP).

Het CBP ziet toe op de doorwerking van de gestelde normen in de praktijk en is bevoegd voorlichting te geven over de wet, de regering te informeren, gedragscodes te toetsen, klachten te behandelen, te bemiddelen en audits uit te voeren bij bedrijven en (semi)overheidsinstellingen. Daarnaast is het CBP bevoegd bestuursdwang toe te passen of een bestuurlijke boete op te leggen. Het college beslist ook over vrijstellingen als het gaat om de verplichte melding van registraties. In principe komt het CBP pas in actie indien een burger vindt dat iemand ten onrechte over zijn gegevens beschikt of er niet zorgvuldig mee omgaat. Hij heeft dan de mogelijkheid om het CBP of de rechter in te schakelen. Wordt de stap naar het CBP genomen, dan kan deze een uitspraak doen over de ingediende klacht. Het CBP kan ook zelf een onderzoek instellen.



## 3 Intern toezicht op verwerking van gegevens

De wet biedt de mogelijkheid om een interne toezichthouder aan te stellen, de 'functionaris voor de gegevensbescherming'. Dit is overigens niet verplicht. Deze functionaris kan bij een andere organisatie werkzaam zijn en houdt onafhankelijk toezicht op de toepassing en naleving van de wet. Hieronder kan worden verstaan:

- toezicht houden;
- inventariseren van gegevensverwerkingen;
- het bijhouden van meldingen van gegevensverwerkingen;
- klachtenbehandeling;
- voorlichting;
- het ontwikkelen van interne regelingen;
- adviseren over technologie en beveiliging.

Het uitoefenen van onafhankelijk toezicht brengt met zich mee dat de functionaris een staffunctie bekleedt, het liefst zo dicht mogelijk bij het management. De verwerker moet ervoor zorgen dat de functionaris zijn werkzaamheden goed kan doen. Het mag niet zo zijn dat hij door gebrek aan faciliteiten wordt belemmerd bij zijn taakuitoefening. De functionaris voor de gegevensbescherming moet bij het CBP worden aangemeld.



## 4 Verwerking van gegevens in de schoolpraktijk

In het onderwijs komen het bestuur en de school bijna dagelijks met de WBP in aanraking. Bij het aanstellen of benoemen van personeel, het in- en uitschrijven van leerlingen, het afnemen van examens, de omgang met ouders en informatieverstrekking aan de overheid speelt de wet een grote rol.

### Sollicitatiebrief

Zodra de sollicitatiebrief - digitaal of schriftelijk - door het schoolbestuur is ontvangen, treedt de WBP in werking. In het Vrijstellingsbesluit is aangegeven hoe met de gegevens van sollicitanten moet worden omgegaan. Blijft de werkgever binnen de aangegeven kaders, dan is er niets aan de hand. Uit de praktijk echter blijkt dat maar weinig werkgevers bekend zijn met de regels. In het Vrijstellingsbesluit staat wie zich met de sollicitatiebrief mogen bemoeien, hoe omgegaan moet worden met de aantekeningen tijdens het sollicitatiegesprek en hoelang de sollicitatiebrief bewaard mag worden. Voor deze gegevens geldt dat ze uiterlijk vier weken na de sollicitatieprocedure moeten worden verwijderd, behoudens de gegevens van de persoon die wordt aangenomen. De gegevens van een sollicitant kunnen maximaal één jaar worden bewaard als de sollicitant daar uitdrukkelijk toestemming voor geeft. Wordt hiervan afgeweken, dan dient het CBP hiervan op de hoogte te worden gesteld.

### Sollicitatiecode

Binnen het primair onderwijs maakt de sollicitatiecode onderdeel uit van de cao. In het voortgezet onderwijs is dat niet het geval, maar veel besturen maken er wel gebruik van. In een sollicitatiecode is geregeld hoe wordt omgegaan met de sollicitant, bijvoorbeeld wie bij de gesprekken aanwezig zijn, hoeveel personen de sollicitatiegesprekken voeren en binnen welke termijnen er wordt gereageerd. Wordt de sollicitant aangenomen, dan treedt een reeks van vrijstellingsbesluiten in werking. Deze zijn van toepassing bij de automatische verwerking van de gegevens (digitaal), de verwerking van de personeelsgegevens en de salarisadministratie. Hiervoor zijn drie aparte vrijstellingsbesluiten opgesteld: het Vrijstellingsbesluit WBP, het Meldingsbesluit WBP en het Besluit kostenvergoeding rechten betrokkene WBP.

### Personeelsdossier

Hierin zijn in eerste instantie de naam-, adres- en woonplaatsgegevens (n.a.w.-gegevens) opgenomen, maar in de loop der tijd zullen ook andere documenten worden toegevoegd. Gedacht kan worden aan wijzigingen in de privésituatie, maar ook aan functionerings- en beoordelingsgesprekken.

Meestal zijn er twee dossiers: het bestuursdossier voor de salarisbetalingen en de Belastingdienst en



het schooldossier voor de verslaglegging van de functionerings- en beoordelingsgesprekken. Beide dossiers dienen goed te worden afgeschermd, zodat onbevoegden geen inzage in de dossiers hebben en er geen stukken uit kunnen worden verwijderd. In het personeelsdossier mogen in beginsel geen medische gegevens worden opgenomen. In het kader van de reïntegratie- en verzuimbegeleiding dient het bestuur zich te beperken tot de informatie over de functionele beperkingen van de zieke werknemer en de noodzakelijke aanpassingen op de werkvloer. Een voorbeeld hiervan is een aangepaste stoel.

### **Recht op correctie, inzage en verzet**

Bij wijzigingen in de privésituatie heeft de werknemer het recht tot correctie. Ook heeft hij het recht om, met redelijke tussenpozen, de werkgever te verzoeken inzage te verstrekken in de persoonsgegevens die worden gebruikt. De werkgever dient binnen vier weken een overzicht van de gegevens aan de werknemer te verstrekken. De werkgever moet daarbij ook informatie geven over het doel van de verwerking(en), de ontvangers van de gegevens en de herkomst ervan. Voor het geven van deze informatie kan de werkgever hoogstens € 5,- vragen.

Na inzage kan de werknemer de werkgever verzoeken de gegevens te verbeteren, aan te vullen, te ver-

wijderen of af te schermen. Dat kan als de gegevens feitelijk onjuist, onvolledig of niet ter zake dienend zijn voor het doel of doeleinden van de verwerking. Bij inwilliging van het verzoek moeten andere organisaties aan wie de (onjuiste) gegevens zijn verstrekt, van de wijziging op de hoogte worden gesteld, tenzij dat onmogelijk is of voor de werkgever een onredelijke inspanning vergt.

De werkgever mag het verstrekken van de gegevens aan de betrokkene weigeren als dat bijvoorbeeld noodzakelijk is in het belang van voorkoming, opsporing en vervolging van strafbare feiten of ter bescherming van de rechten en vrijheden van anderen. De werknemer heeft het recht van verzet. Dit houdt in dat hij het recht heeft bezwaar te maken (verzet aan te tekenen) tegen bepaalde vormen van gebruik van zijn gegevens door de werkgever. Er zijn twee vormen van verzet: verzet bij direct marketing en verzet wegens bijzondere persoonlijke omstandigheden (bijvoorbeeld ten aanzien van medische gegevens). Zodra door de werknemer verzet wordt aangetekend tegen het gebruik van zijn gegevens voor marketing- en charitatieve doeleinden, moet de werkgever dat gebruik altijd direct beëindigen.

Zoals genoemd kan een werknemer ook verzet aantekenen wegens bijzondere persoonlijke omstandigheden. De werkgever moet beslissen of hij stopt met

de verwerking of hiermee doorgaat, omdat hij meent hiervoor een goede reden te hebben.

De werkgever mag doorgaans een vergoeding van ten hoogste € 4,50 vragen om het verzoek in behandeling te nemen. Dit geld moet hij weer teruggeven als hij het verzoek inwilligt.

### **Klachtrecht werknemer**

De werknemer kan een klacht bij het CBP indienen over de verwerking van zijn persoonsgegevens. Voor dat hij dit doet, moet eerst de werkgever schriftelijk in de gelegenheid worden gesteld op de klacht te reageren. Pas als de werkgever niet binnen de door de werknemer gestelde termijn reageert, kan de klacht aan het CBP worden voorgelegd. Na ontvangst van de klacht stelt het CBP eerst vast of het bevoegd is de klacht te behandelen. Daarbij is een belangrijk criterium dat het gaat om gebruik van persoonsgegevens waarop de WBP van toepassing is. Ook als het CBP bevoegd is, kan het besluiten de klacht niet in behandeling te nemen. Dit gaat bijvoorbeeld op als de overtreding van de werkgever niet ernstig genoeg is, als er al herstel of genoegdoening door de werkgever is aangeboden of als het om een zo ernstige zaak gaat, dat het beter is deze direct aan de rechter voor te leggen.

Als het CBP de klacht behandelt, wordt die in een

brief met een aantal vragen aan de werkgever voorgelegd met het verzoek deze binnen een bepaalde termijn (meestal drie weken) te beantwoorden. De werkgever ontvangt in de regel van alle correspondentie tussen de werknemer en het CBP een kopie. De werknemer ontvangt meestal kopieën van de reacties van de werkgever. Als de werkgever nieuwe zaken aan de orde stelt, zal het CBP indien nodig de werknemer om commentaar vragen.

Als alle relevante informatie beschikbaar is en beide partijen hun standpunt voldoende duidelijk hebben gemaakt, zal het CBP in de regel een rapport maken met voorlopige bevindingen. Dit worden aan beide partijen voorgelegd met het verzoek daar binnen twee weken op te reageren. Het CBP maakt daarna zijn eindrapport. Daarin zijn de bevindingen van het onderzoek, een conclusie over de voorgelegde klacht en eventueel een aanbeveling opgenomen. Deze aanbeveling is niet bindend. De uitspraken kunnen geanonimiseerd openbaar worden gemaakt. Vaak is een rapport met bevindingen van het CBP voldoende om een klacht naar tevredenheid af te handelen, maar het komt ook voor dat de werkgever het advies van het CBP niet opvolgt. Als de werkgever weigert om verwerkingen, die in strijd zijn met de wet, te beëindigen of te wijzigen, beschikt het CBP over de bevoegdheid om indien nodig handhaving van wet-

telijke regels af te dwingen. Het CBP heeft niet de bevoegdheid een schadevergoeding toe te kennen. Aangezien de rechter deze bevoegdheid wel heeft, kan de werknemer overwegen om de zaak aan de rechter voor te leggen. De werknemer kan ook bij de rechtbank vragen om de werkgever een bevel te geven. De rechter kan hem bijvoorbeeld gebieden maatregelen te nemen tot herstel van de gevolgen van een bepaalde handeling van de werkgever. In beide gevallen zal de werknemer een advocaat moeten inschakelen.

### **Overdracht van gegevens bij fusie**

Bij een faillissement, fusie of overname mag het schoolbestuur personeelsdossiers overdragen aan een ander schoolbestuur. Voorwaarde is wel dat het overdragende schoolbestuur zich houdt aan de volgende waarborgen om de privacybelangen van zijn werknemers te beschermen:

- het bestuur dient de overdracht aan te kondigen in een daarvoor geschikt medium. Bij voorkeur gebeurt dit per brief en bijvoorbeeld ook in het personeelsblad en/of op het intranet;
- de werknemers krijgen de mogelijkheid bepaalde gegevens te laten verwijderen en bezwaar aan te tekenen tegen de overdracht. Indien geen bezwaar is aangetekend, kan worden uitgegaan van veronderstelde toestemming van de werknemer voor de overdracht;
- het bestuur mag niet méér gegevens verstrekken dan noodzakelijk is voor de uitvoering van de arbeidsovereenkomst of een publiekrechtelijke aanstelling als ambtenaar. Het bestuur zal daarom alle personeelsdossiers moeten opschonen en alle oude en niet meer relevante gegevens moeten verwijderen. Zo is een verslag van een functioneringsgesprek van tien jaar geleden niet meer relevant.



## 5 Verwerking van gegevens voor leerlingenadministratie

<sup>2</sup> WPO = Wet op het primair onderwijs, WEC = Wet op de expertisecentra, WVO = Wet op het voortgezet onderwijs

<sup>3</sup> OCW = ministerie van Onderwijs, Cultuur en Wetenschap

In de onderwijswetgeving (WPO, WEC, WVO<sup>2</sup>) staat wanneer leerlingen toegelaten kunnen/moeten worden tot de school. Het toelaten is formeel een zaak van het bestuur, maar in de praktijk komt het erop neer dat de scholen dit zelf regelen. In de bekostigingsbesluiten van de onderwijswetten wordt aangegeven hoe de administratie moet plaatsvinden. Dit zijn wettelijke voorschriften die mede bepalend zijn voor de bekostiging van het onderwijs. Binnen het onderwijs geldt ook het onderwijsnummer voor een leerling. Voor het toepassen van het onderwijsnummer is door het ministerie van OCW<sup>3</sup> en de besturen-organisaties het model 'Privacyreglement Verwerking leerlingengegevens' opgesteld (dit reglement kunt u downloaden van [www.vosabb.nl](http://www.vosabb.nl)).

Het Vrijstellingsbesluit geeft aan dat de gegevens van de leerlingen tot twee jaar na het verlaten van de school bewaard moeten worden. Het Bekostigingsbesluit WPO geeft echter aan dat de gegevens vijf jaar na het verlaten van de school bewaard moeten blijven en dat vervolgens binnen acht weken de gegevens vernietigd moeten worden. In het Vrijstellingsbesluit wordt meestal onder de term 'bewaartermijn' aangegeven: 'langer bewaren van de gegevens is alleen toegestaan als de persoonsgegevens noodzakelijk zijn ter voldoening aan een wettelijke

bewaarplicht'. In dit geval heeft het Beskostigingsbesluit WPO voorrang.

In het kader van de Leerplichtwet 1969 heeft de leerplichtambtenaar de bevoegdheid om leerlingengegevens te controleren.

### Inzage in leerlingendossier

Regelmatig worden scholen door ouders benaderd met de vraag of zij het dossier van het kind kunnen inzien of dat het onderwijskundig rapport aan hen kan worden voorgelegd, voordat het aan de nieuwe school wordt verzonden. Het inzien van een leerlingdossier dient in ieder geval, met redelijke tussenpozen, te worden toegestaan. Als een kopie gevraagd wordt van een bepaald rapport, kan die worden gemaakt. Het is verstandig om tijdens het kopiëren het dossier mee te nemen om te voorkomen dat andere documenten eruit worden gehaald. Persoonlijke aantekeningen van bijvoorbeeld de leerkracht mogen bij het kopiëren worden afgedekt. De ouders hoeven namelijk niet in te stemmen met een onderwijskundig rapport. De wet schrijft voor dat het rapport alleen in afschrift moet worden verstrekt. De basisschool dient de ouders uiterlijk op het moment dat het onderwijskundig rapport aan de ontvangende school voor voortgezet onderwijs wordt verstrekt, over dit rapport te informeren. Ook handelingsplannen, psy-

chische rapporten en adviezen dienen op aanvraag in principe te worden verstrekt.

### **Verstrekken van gegevens aan ouders**

Ouders (of verzorgers) hebben wettelijk het recht geïnformeerd te worden over de vorderingen van hun kind. In de meeste gevallen levert dit geen probleem op. Dit kan wel het geval zijn als ouders gaan scheiden of gescheiden zijn, vooral als de niet met het gezag belaste ouder geïnformeerd wil worden en de andere ouder zich daartegen verzet. Na hun echtscheiding zijn sinds een wetwijziging per 1 januari 1998 in principe beide ouders met het gezag over hun kind belast (co-ouderschap). In die gevallen hebben beide ouders wat betreft de informatievoorziening over hun kind gelijke rechten. Soms bepaalt de rechter op verzoek van een van de ouders dat het gezag niet aan beide ouders, maar slechts aan een van hen wordt toegekend. Op grond van artikel 377 b, boek I van het Burgerlijk Wetboek is de ouder die alleen met het gezag is belast, gehouden om de andere ouder op de hoogte te stellen over belangrijke aangelegenheden met betrekking tot de persoon en het vermogen van het kind en deze te raadplegen. De rechter kan deze bepaling buiten toepassing laten als het belang van het kind dat vereist. Onverminderd deze bepaling wordt de niet met het gezag belaste

ouder op zijn verzoek door derden, die beroepshalve beschikken over informatie over belangrijke feiten en omstandigheden, die de persoon van het kind of diens verzorging en op voeding treffen, daarvan op de hoogte gesteld. Dit is bepaald in artikel 377 c van het Burgerlijk Wetboek. Zo'n derde, zoveel zal duidelijk zijn, is de school waar het kind onderwijs volgt. De school is niet verplicht die informatie te verschaffen, indien de informatie ook niet aan de met het gezag belaste ouder zou worden verschaft of het belang van het kind zich tegen het verschaffen van de informatie verzet. In met name het laatste geval zal een school soms een lastige beslissing moeten nemen om niet ingeklemd te raken tussen de ene ouder die de informatie wenst en de andere ouder, die deze informatieverstrekking in strijd met het belang van het kind acht. Indien de school besluit om de gevraagde informatie te weigeren, kan de rechter op verzoek van de niet met het gezag belaste ouder bepalen, dat de informatie op de door de rechter te bepalen wijze moet worden verstrekt. De rechter wijst het verzoek in ieder geval af als het belang van het kind zich tegen het verschaffen van de informatie verzet.

Geadviseerd wordt om een beleidsstuk op te stellen waarin staat hoe het bestuur/de school hiermee omgaat.

### Verstrekking gegevens aan derden

Veel instanties doen een beroep op scholen met het verzoek nadere informatie te verstrekken. Uitgangspunt is dat het bestuur/de school deze gegevens niet zonder toestemming kan verlenen. Zo vragen gemeenten gegevens op voor het verstrekken van subsidie of willen ze de Cito-scores weten. (Leerling) gegevens kunnen slechts geanonimiseerd worden verstrekt.

Ook verzekeringsmaatschappijen, charitatieve instellingen en andere organisaties doen graag een beroep op scholen om leerlinggegevens te krijgen. Zonder toestemming mogen deze niet worden verstrekt. Anders is het als de Belastingdienst gegevens opvraagt. Besturen/scholen zijn dan wel verplicht de gegevens te verstrekken, mits dit is gebaseerd op wet- en regelgeving. De Belastingdienst heeft geen recht van spreken als het bijvoorbeeld gaat om het verzenden van een folder of brochure.

In het kader van onderzoeken kunnen scholen ook benaderd worden voor medewerking. Als voorbeeld kunnen genoemd worden de Raad voor de Kinderbescherming, politie en justitie. Formeel is het zo geregeld dat zonder meer medewerking moet worden verleend bij een justitieel onderzoek. Het is echter de vraag of ook medewerking moet worden verleend

aan een onderzoek door bijvoorbeeld de politie naar een personeelslid. Voor het voorkómen of opsporen van strafbare feiten, is het bestuur alleen verplicht deze gegevens te verstrekken indien de politie hier uitdrukkelijk en gericht om vraagt én aangeeft op grond van welke wettelijke regeling het bestuur de gegevens moet verstrekken. Dit kan bijvoorbeeld op bevel van de rechter-commissaris in strafzaken. Advocaten hoeven niet te worden toegelaten. Voor het verstrekken van informatie aan een incassobureau, naar aanleiding van een schuld van een werknemer, dient het bestuur toestemming van de betrokkene te hebben. Dit is anders bij beslaglegging. In dat geval kan het zijn dat de werkgever wettelijk verplicht is de verlangde informatie te verschaffen.

**NB: hoewel de WBP niet direct op de situatie van illegaal in Nederland verblijvende leerlingen van toepassing is, dient te worden vermeld dat op grond van wettelijke bepalingen illegale leerlingen niet tot het onderwijs mogen worden geweigerd.**



## 6 Foto's, video-opnamen, webcam en internet

Op schoolfeestjes worden veel foto's gemaakt. Meestal jaarlijks laten scholen van de leerlingen school- en klassenfoto's maken. Ook willen scholen graag op internet laten zien wat er allemaal gebeurt.

Het is verstandig om bij de aanmelding van leerlingen aan de ouders te vragen hen schriftelijk te laten verklaren of zij bezwaar hebben tegen het maken van foto's en video-opnamen. Het is aan te bevelen een aparte verklaring van klassenfoto's te vragen, omdat er anders een probleem kan ontstaan als ouders negatief op het eerste verzoek reageren. Ook dient toestemming te worden gevraagd voor het plaatsen van foto's op internet.

Indien geen toestemming wordt verkregen, dient de school zorgvuldig om te gaan met de publicatie van foto's en video-opnamen. De leerlingen om wie het gaat, moeten als het ware onzichtbaar worden gemaakt en uit video-opnamen worden geknipt. Het plaatsen van beelden van deze leerlingen op internet zonder toestemming is uit den boze. Er zijn gevallen bekend waarin misbruik is gemaakt van foto's op internet. Met de digitale knip- en plakfuncties is het een fluitje van een cent om beelden zo te bewerken dat er een geheel andere situatie wordt gecreëerd. Leerlingen zouden hiermee kunnen worden gepest en er psychische schade door kunnen ondervinden.

Wel dient onderscheid te worden gemaakt tussen intern internet (intranet) en extern internet. Voor intern gebruik is het bezwaar niet altijd van toepassing. De werkgever mag bijvoorbeeld de naam en de functie van de werknemer op het intranet plaatsen. Anders is het bij het plaatsen van een foto op het intranet. In dat geval zal de werknemer toestemming moeten geven. Het bezwaar is niet van toepassing bij het gebruiken van een webcam als deze alleen binnen de school wordt gebruikt. De beperkingen gelden wel als de opnamen ook extern te zien zijn.

In toenemende mate wordt door leerlingen misbruik gemaakt van kleine camera's en mobieltjes met foto- en filmfunctie. Ze maken stiekem foto's en/of filmpjes en zetten die op internet. Wanneer er daadwerkelijk foto's en/of filmpjes op internet worden gezet, is er sprake van schending van de privacy van degene die is gefotografeerd/gefilmd. Alleen de persoon in kwestie kan aangifte doen, niet de school.

Voor alle onderdelen geldt dat het bestuur hiervoor beleid moet hebben en dat via de schoolgids aan de ouders bekendmaakt. Als er geen beleid is ontwikkeld en er ontstaan rechtszaken, dan is het schoolbestuur in de meeste gevallen de verliezende partij. Dit kan financiële gevolgen hebben, bijvoorbeeld als



## 7 Controle e-mail en internetgebruik

ouders een beroep doen op het portretrecht.

In scholen worden ook steeds meer camera's als beveiligingsmiddel ingezet. Meestal dienen deze camera's als veiligheid voor personeel en leerlingen. Als met tekstborden wordt aangegeven dat camera-beveiliging plaatsvindt, is dit meestal voldoende. Het toepassen van verborgen camera's is in principe niet toegestaan. In zeer uitzonderlijke situaties is een verborgen camera toegestaan, mits voorafgaande toestemming van het Openbaar Ministerie is verkregen in het belang van een eventueel onderzoek. Er moet in dat geval sprake zijn van een concrete verdenking, waarvan de gedragingen niet anders dan met behulp van een camera kunnen worden vastgesteld.

Het schoolbestuur mag als werkgever voorwaarden stellen aan het gebruik van e-mail en internet of bepaalde soorten gebruik verbieden. Vervolgens mag het bestuur bij een vermoeden van misbruik onder bepaalde voorwaarden een controle uitvoeren. Indien het schoolbestuur het gebruik van e-mail en internet wil controleren, dan moet het aan de volgende voorwaarden voldoen:

- De controle moet in een redelijke verhouding staan tot de belangen van de werknemers.
- Het schoolbestuur moet de controle melden bij het CBP. Alleen als de medezeggenschapsraad met de controle heeft ingestemd, hoeft dat niet.
- Het schoolbestuur moet de werknemers informeren over de regels voor het gebruik van e-mail en internet. Dit betekent dat werknemers moeten weten wat wel en niet mag, dat controle mogelijk is en op welke manier dat gebeurt.
- Het schoolbestuur moet rekening houden met het recht op vertrouwelijke communicatie.
- Het schoolbestuur moet de controle van e-mail en internet vooraf met de medezeggenschapsraad bespreken.
- Voordat het schoolbestuur met de controle begint, moet het het doel bepalen waarvoor de controle noodzakelijk is. Van dit doel hangt namelijk af hoe omvangrijk de controle mag zijn en



op welke manier die mag gebeuren. Een doel kan bijvoorbeeld zijn: systeem- en netwerkbeveiliging of het verminderen van kosten en tijdsverlies.

Indien het schoolbestuur geen gedragsregels of protocol voor het gebruik van e-mail en internet op het werk heeft, dan gelden algemene regels. Het bestuur kan privégebruik van e-mail en internet onder werktijd niet helemaal verbieden. De werknemer dient zelf rekening te houden met de inhoud van de e-mail en de websites die hij bezoekt. Het schoolbestuur is gerechtigd zakelijke e-mail te lezen van een werknemer, ook als hij niet aanwezig is. Als uit het onderwerp van een e-mail blijkt dat het bericht van persoonlijke aard is, dan mag het bestuur dat bericht niet controleren. Blijkt een scheiding tussen zakelijke en privémail niet mogelijk, dan moet het schoolbestuur er rekening mee houden dat werknemers privéberichten ontvangen en versturen. Bij controle dient het bestuur de privéberichten zo veel mogelijk te ontzien.

Leerlingen mogen niet zonder meer worden gecontroleerd tijdens hun internetgebruik. Ook zij moeten hiervan op de hoogte worden gebracht. Volgens de WBP mogen gegevens alleen worden verzameld voor welbepaalde en gerechtvaardigde doelen. Controle op internetgebruik van leerlingen is dus

toegestaan, mits er duidelijke regels zijn opgesteld en er wordt aangegeven dat er wordt gecontroleerd. Doelen kunnen bijvoorbeeld zijn: systemen en netwerkbeveiliging, tegengaan van seksuele intimidatie/discriminatie en naleven van afspraken over verboden gebruik.



## 8 Computerapparatuur

Het is aan te bevelen beleid te formuleren voor het omgaan met computerapparatuur binnen de school. Het is regelmatig voorgekomen dat vertrouwelijke informatie uit computers is gebruikt om er bijvoorbeeld zelf beter van te worden. Het bestuur/de school dient met name beleid op te stellen voor personeelsleden die met het onderhoud van de apparatuur te maken hebben. Dit kan bijvoorbeeld door de betrokkenen een contract te laten ondertekenen, waarin zij verklaren vertrouwelijk met de verkregen informatie om te gaan.

Daarnaast wordt aanbevolen om ook voor het gebruik van computers binnen de school beleid op te stellen. Het gaat dan met name over het bezoeken van websites (met name welk soort sites niet geopend mogen worden) en de controle daarop.



## 9 Zorg- en adviesteam

Binnen de school of bovenschools wordt er regelmatig gebruikgemaakt van zorg- en adviesteams (ZAT's). Het is van belang dat het ZAT beschikt over een privacyreglement, waarin rekening wordt gehouden met de aanwezigheid en deelname in een ZAT. De gegevens die worden verwerkt in een ZAT, moeten een bepaald doel voor ogen hebben. Ze moeten in het belang zijn van de individuele leerling en van zijn of haar optimale schoolloopbaan. Een gevolg van dit doel kan zijn dat vaak niet het gehele leerlingdossier ingebracht kan worden in het ZAT. Als een leerling die goed presteert sociaal-emotionele problemen heeft, hoeven de cijfers niet in het ZAT te worden ingebracht.

Naast het doel dient er ook een aanleiding te zijn om de gegevens te verwerken in het ZAT. De persoonsgegevens van de leerling kunnen alleen besproken worden in het ZAT als er sprake is van ondubbelzinnige toestemming van de ouders of de leerling (vanaf 16 jaar) en/of als het belang van de leerling in het geding is. Dit is bijvoorbeeld het geval als er sprake is van een bedreigende opvoedingssituatie.

Vaak wordt er in de praktijk een brief gestuurd naar de ouders/verzorgers van de leerling met de mededeling dat er een voornemen bestaat om de leerling te bespreken in het ZAT. Als de ouders hier geen be-



## 10 Gegevensverwerking bij een zieke werknemer

zwaar tegen maken, kan de leerling worden besproken, maar alleen wat betreft de gegevens die van direct belang zijn bij de toelichting op de vraagstelling van die betreffende leerling. Als er geen instemming wordt verleend, kan een leerling anoniem in het ZAT worden besproken.

Voorts kan het zo zijn dat in het kader van de pedagogische taakstelling de school een gerechtvaardigd belang heeft om persoonsgegevens van leerlingen te verwerken in een intern zorgteam. De deelnemers in dit interne zorgteam moeten wel belast zijn of nauw betrokken zijn met het geven van onderwijs en het begeleiden van de betreffende leerling. Het verschil tussen een intern zorgteam en een ZAT bestaat uit de interventies die eruit voortkomen. Pas wanneer het maatregelen betreft die ook betrekking kunnen hebben op de wereld buiten de school, uitgevoerd door partijen buiten de school, is er sprake van een ZAT. Wel blijft ook bij het interne zorgteam van belang dat toestemming van de leerling wenselijk kan zijn. Meer informatie staat in de 'Handreiking verwerking persoonsgegevens in zorg- en adviesteams' van het Nederlands Jeugdinstituut. U vindt deze publicatie onder andere op [www.rijksoverheid.nl](http://www.rijksoverheid.nl) en [www.zat.nl](http://www.zat.nl).

Als een werknemer ziek wordt, is het van belang dat de werkgever op de hoogte is van de gegevens die hij mag opvragen en verwerken. De werkgever mag nooit zelf vragen wat de aard en oorzaak van de ziekte is. De volgende informatie kan de werkgever wel opvragen bij de werkgever: adres waar hij verblijft, telefoonnummer, vermoedelijke duur van het verzuim, lopende afspraken en werkzaamheden, of de ziekte verband houdt met een arbeidsongeval (maar dus niet of het werkgerelateerd is), of de werknemer onder de vangnetbepalingen van de Ziektewet valt en of er sprake is van een verkeersongeval waarbij een derde wellicht aansprakelijk kan worden gesteld (in verband met het mogelijke verhaalsrecht).

De bedrijfsarts mag de werkgever wel informeren over ziekteverzuim dat werkgerelateerd is, mits dit noodzakelijk is voor de re-integratie van de werknemer. De overige informatie die de bedrijfsarts mag verstrekken aan de werkgever moet noodzakelijk zijn voor de beoordeling van de verzuimbegeleiding, de loondoorbetalingsverplichting en de re-integratie. Als de bedrijfsarts andere informatie wil verstrekken aan de werkgever, dient de werknemer daar toestemming voor te geven.

Als de re-integratie heeft aangevangen, zal de zieke werknemer aan de arbodienst/bedrijfsarts informatie

moeten verschaffen die noodzakelijk is voor de re-integratie. Ook de werkgever zal informatie moeten verschaffen aan de arbodienst/bedrijfsarts. Vooraf moet aan de werknemer worden aangegeven welke gegevens de werkgever verstrekt en met welk doel hij dat doet (controle, re-integratie etc).

In de verzuimoverzichten die de werkgever opstelt, mogen geen medische gegevens worden opgenomen waaruit kan worden afgeleid welke werknemer het betreft. De individuele verzuim informatie mag alleen worden verwerkt door werknemers die direct betrokken zijn bij het verzuimbeleid. Meer informatie staat in de publicatie 'De zieke werknemer en privacy' van het CBP. U vindt deze publicatie op [www.cbpweb.nl](http://www.cbpweb.nl).

### **Bewaartermijnen**

Het re-integratiedossier van de werknemer dient na het einde van het dienstverband zo snel mogelijk te worden vernietigd, behalve bij scholen die eigenrisicodrager zijn. De persoonsgegevens met betrekking tot het verzuim mogen niet langer dan twee jaar na het einde van het dienstverband worden bewaard, behoudens een langere wettelijke bewaartermijn. Een afgesloten re-integratiedossier mag maximaal twee jaar worden bewaard. Als er een grote kans bestaat op terugval, mag het re-integratiedossier maximaal vier jaar worden bewaard.



## 11 Persoonsgebonden nummer bij uitwisseling leerling- en begeleidingsgegevens

Op 1 augustus 2012 zijn er wijzigingen<sup>4</sup> in de onderwijswetten in werking getreden die van invloed zijn op gegevensuitwisseling. Het gaat hier om het gebruik van het persoonsgebonden nummer (pgn) van een leerling of deelnemer voor het uitwisselen van gestandaardiseerde leer- en begeleidingsgegevens tussen scholen en instellingen voor primair onderwijs, voortgezet onderwijs en educatie en beroepsonderwijs. Onder leergegevens wordt verstaan: gegevens over de leerloopbaan en de leerresultaten van de leerling, zoals gevolgd onderwijs, behaalde diploma's, examencijfers, rapportcijfers, gevolgde stages en behaalde certificaten (typediploma, digitaal rijbewijs enz.). Onder begeleidingsgegevens kunnen meerdere typen gegevens worden verstaan. Enerzijds kan het gaan om extra begeleiding die een leerling heeft gekregen in verband met bijvoorbeeld dyslexie of faalangst. Anderzijds kan het gaan om extra uitdagingen, die aan een leerling zijn geboden in verband met zijn hoge begaafdheid, zonder welke uitdagingen de desbetreffende leerling zich wellicht over de hele linie minder zou hebben ingespannen dan wenselijk was geweest. Ook kan begeleiding nodig zijn geweest in verband met ingrijpende familieomstandigheden, die aan de basis lagen van tijdelijk terugvallende schoolprestaties. Het gaat uitsluitend om begeleidingsgegevens, die direct samenhangen

met het leerproces.

Verder regelen de gewijzigde bepalingen dat het pgn in het verkeer tussen het bevoegd gezag van scholen voor (voortgezet) speciaal onderwijs en de Informatie Beheer Groep kan worden gebruikt bij de opgave van de leerlingen die door deze scholen ambulantly worden begeleid. Deze opgave vindt plaats ten behoeve van de vaststelling van het budget voor personeels- en arbeidsmarktbeleid van de begeleidende school. Met de wetswijzigingen is het gebruik van het pgn in het onderwijs derhalve uitgebreid. In het Besluit uitwisseling leer- en begeleidingsgegevens wordt nader gespecificeerd welke leergegevens en direct met het leren samenhangende begeleidingsgegevens ten hoogste door scholen onderling over een leerling mogen worden uitgewisseld, met behulp van het pgn ten behoeve van de in- en uitschrijving van die leerling.

### Overstapservice Onderwijs

Het besluit biedt ruimte voor verschillende vormen van elektronische uitwisseling van gegevens tussen scholen. Daaronder valt ook de uitwerking van een standaard en een overstapservice. Van deze overstapservice kan gebruik worden gemaakt via aanmelding bij de overstapservice Onderwijs (OSO, zie [www.overstapserviceonderwijs.nl](http://www.overstapserviceonderwijs.nl)).

---

<sup>4</sup> Wijziging van de Wet op het primair onderwijs, de Wet op de expertisecentra, de Wet op het voortgezet onderwijs, de Wet educatie en beroepsonderwijs en de Wet verzelfstandiging Informatiseringsbank in verband met het gebruik van het persoonsgebonden nummer bij onder meer de uitwisseling van leer- en begeleidingsgegevens van leerlingen.



## 12 Sociale media

De OSO is het geheel van afspraken, standaarden en beveiligde verbindingen die de veilige digitale overdracht van studie- en begeleidingsgegevens van een leerling vanuit de leerlingadministratie van de huidige school naar de nieuwe school faciliteert. Binnen OSO genereert de huidige school een digitaal overstapdossier binnen de eigen en bestaande leerlingadministratiesoftware. De nieuwe school kan op haar beurt binnen haar leerlingadministratiesoftware een overstapdossier via OSO opvragen. Indien aan alle eisen en voorwaarden van de aanvraag is voldaan, stelt het OSO-systeem een eenmalige beveiligde verbinding tussen beide scholen beschikbaar, waarmee het dossier wordt overgebracht. De nieuwe school kan het daarna in het eigen systeem verwerken. Deze digitale uitwisseling is sneller en minder gevoelig voor fouten dan uitwisseling door middel van papieren dossiers. Het verlicht tevens de administratieve last op scholen. Uniek is dat in het OSO-overdrachtsproces geen centrale opslag van leerlinggegevens plaatsvindt.

Bij het verwerken van persoonsgegevens op internet, en daarbij in sociale media, dient rekening te worden gehouden met de WBP. Het is ook van belang dat er wordt gekeken of de publicatie van persoonsgegevens een legitiem doel dient en of dat overeenkomt met het doel waarvoor de persoonsgegevens in eerste instantie zijn verkregen.

Zowel in het voortgezet onderwijs als in het primair onderwijs is in de afgelopen jaren een sterke toename geweest van communicatie via sociale media, zoals Facebook, Hyves en Twitter. Daar kunnen risico's aan verbonden zijn, zoals het verkleinen van de professionele afstand tussen leerkrachten en leerlingen die via sociale media contact met elkaar hebben. Dit kan ertoe leiden dat de professionele relatie tussen leerkracht en leerling in gevaar komt en dat in de digitale wereld de scheiding tussen school en privé vertroebeld raakt. Het is daarom aan te raden om als leerkracht of als school een apart deel in sociale media op te zetten dat voor het werkdomein bedoeld is. Daarin kunnen schoolge-relateerde onderwerpen worden besproken en treedt de privérelatie tussen de leerkracht en leerling niet of veel minder op de voorgrond. Leerkrachten dienen op sociale media zelf deze grens te bewaken tussen wat wel of niet professioneel is

Een leerkracht vervult een voorbeeldfunctie. Dit bete-



## 13 Tot besluit

kent dat privé-uitlatingen via sociale media of afbeeldingen die hierop worden geplaatst, niet alleen de leerkracht kwetsbaar kunnen maken, maar ook het imago van de school kunnen raken. Om dit soort risico's tot een minimum terug te dringen, is het aan te raden om binnen de organisatie een protocol op te stellen voor het omgaan met sociale media. Dit protocol is van toepassing op alle betrokkenen, dus leerlingen en personeelsleden. Een modelprotocol voor het gebruik van sociale media staat op [www.vosabb.nl](http://www.vosabb.nl) (downloads > modellen).

Het kan ook verstandig zijn om regels op te stellen voor het gebruik van mobiele telefoons op school en in de klas. Smartphones geven met één klik toegang tot sociale media. Een afbeelding of opname vanuit de klas kan razendsnel op het wereldwijde netwerk belanden. Het is van belang om hierbij te vermelden dat de Landelijke Klachtencommissie (LKC) hier uitlatingen over heeft gedaan. Zo heeft de LKC aangegeven dat mobiele telefoons die om een daartoe moverende reden door de leraar zijn ingenomen, na schooltijd, in principe, weer verstrekt dienen te worden aan leerlingen, aangezien telefonische en digitale bereikbaarheid van groot belang is in de huidige samenleving.

Meer informatie staat op de website van het Project Preventie Seksuele Intimidatie [www.ppsi.nl](http://www.ppsi.nl) (>informatiebladen).

Het is met betrekking tot privacybescherming onmogelijk volledig te zijn. Door snelle (technische) ontwikkelingen rijzen steeds weer nieuwe vraagstukken, die direct of indirect verband houden met privacy. Ook doen zich op dit vlak voortdurend beleidsontwikkelingen voor, zoals het beleid en de daaruit voortvloeiende maatregelen in het kader van de terreurbestrijding.

Daarom is het raadzaam om de hoogte te blijven van recente ontwikkelingen op het gebied van privacy. De website [www.cbppweb.nl](http://www.cbppweb.nl) van het College Bescherming Persoonsgegevens en [www.vosabb.nl](http://www.vosabb.nl) kunnen hiertoe dienstig zijn.



## Colofon

Voor meer informatie over de katernenreeks van VOS/ABB:

zie [www.vosabb.nl](http://www.vosabb.nl) of neem contact op met VOS/ABB via [secretariaatvereniging@vosabb.nl](mailto:secretariaatvereniging@vosabb.nl).

Uitgever: VOS/ABB ©

Samenstelling: mr. José van Snek, juridisch adviseur Helpdesk VOS/ABB

Eindredactie: drs. Martin van den Bogaardt, VOS/ABB,

Vormgeving: MoMuMedia, Schiedam

Woerden, september 2013

Alle rechten voorbehouden. Niets uit deze uitgave mag worden verveelvoudigd, opgeslagen in een geautomatiseerd gegevensbestand, of openbaar gemaakt, in enige vorm of op enige manier, hetzij elektronisch, mechanisch, door fotokopie, opnamen, of enige andere manier zonder voorafgaande schriftelijke toestemming van de uitgever.



Reeds verschenen in de VOS/ABB-katernenreeks:

Katern 1 - Arbobeleid en veiligheid (herziene online versie)

Katern 2 - Wegwijzer Wet bescherming persoonsgegevens (herziene online versie)

Katern 3 - Wet op de Beroepen in het Onderwijs (Wet BIO) (herziene online versie)

Katern 4 - Auteursrechtelijke bijdragen (vervallen)

Katern 5 - Levensloop (inclusief de nieuwe regeling ouderschapsverlofkorting)

Katern 6 - Functiewaardering en FUWA PO

Katern 7 - Toelating en verwijdering leerlingen VO

Katern 8 - Toelating en verwijdering leerlingen PO

Katern 9 - Vervangingsfonds, Participatiefonds en Risicofonds

Katern 10 - Algemene wet bestuursrecht (Awb) (herziene online versie)

Katern 11 - Wegwijzer aanbesteden

Katern 12 - Normtaak en taakbeleid in het primair onderwijs

Katern 13 - Btw-richtlijnen in het onderwijs (geheel herziene druk)

Katern 14 - Aanstellings- en ontslagbeleid

Katern 15 - School en aansprakelijkheid

Katern 16 - Goed onderwijs, goed bestuur

Katern 17 - Stichten van scholen

Katern 18 - Fondsenwerving in het onderwijs

Katern 19 - Educatief partnerschap