

Privacy

Checklist privacy-afspraken voor scholen

Scholen werken met gegevens van en over leerlingen: schoolprestaties, contactgegevens, intakeformulieren, inlogcodes voor digitaal leermateriaal en nog meer. Dat heten persoonsgegevens, en een school is altijd juridisch verantwoordelijk voor het juiste gebruik ervan, ook als daarbij programma's van softwareleveranciers gebruikt worden. En dat is tegenwoordig vrijwel altijd het geval.

Wat die verantwoordelijkheid inhoudt, is onder meer geregeld in de Wet bescherming persoonsgegevens.

Die zegt dat softwareleveranciers 'bewerkers' worden als ze persoonsgegevens opslaan (bijvoorbeeld 'in de cloud') of delen (bijvoorbeeld met leveranciers van educatief materiaal). De afspraken tussen softwareleveranciers en scholen over wat er wel en niet met persoonsgegevens mag gebeuren, worden vastgelegd in een zogeheten bewerkersovereenkomst. De wet legt scholen daarbij een aantal voorwaarden op. In deze flyer een checklist voor scholen om vast te stellen of aan de wettelijke eisen is voldaan.

Met softwareleveranciers moet u in ieder geval de volgende afspraken maken:

<input type="checkbox"/>	Volgens de wet moet er een overeenkomst zijn, liefst een schriftelijke. Is die er?
<input type="checkbox"/>	Het moet duidelijk zijn tussen wie er afspraken zijn, en waar ze bereikt kunnen worden. Zijn de partijen en hun contactgegevens opgenomen? <ul style="list-style-type: none">▪ Is duidelijk wat is de rol van iedere partij? Wie de bewerker is en wie de verantwoordelijke?▪ Zijn er anderen betrokken (bijvoorbeeld subleveranciers): zo ja, noem wie dat zijn en wat hun rol is.
<input type="checkbox"/>	Is beschreven welke gegevens door de leverancier worden verwerkt? <ul style="list-style-type: none">▪ Voeg eventueel een specificatie als bijlage toe.
<input type="checkbox"/>	Is er geregeld dat de leverancier alleen in opdracht en volgens instructies van de school persoonsgegevens verwerkt? <ul style="list-style-type: none">▪ Is er een beschrijving wat de leverancier/bewerker wel en niet mag? Bijvoorbeeld dat de gegevens alleen voor dienstverlening aan de school mogen worden gebruikt?▪ Is vastgelegd dat hetzelfde geldt voor eventueel ingeschakelde subleveranciers?
<input type="checkbox"/>	De leverancier/bewerker hoort gebonden te zijn aan een geheimhoudingsbeding. Is dat er? Is ook vastgelegd dat derden alleen met toestemming van de school toegang krijgen tot de persoonsgegevens? <ul style="list-style-type: none">▪ Is afgesproken dat de school direct geïnformeerd wordt bij een verzoek van derden?
<input type="checkbox"/>	Gegevens mogen niet eindeloos bewaard worden. Is er een bewaartermijn of vernietigings-termijn geregeld, of voorziet de software daarin? Zijn er afspraken gemaakt over het beëindigen van de software/dienst? <ul style="list-style-type: none">▪ Krijgt de school zelf de gegevens aangeleverd of zijn ze te downloaden?▪ Is afgesproken in welk bestandsformaat de school de gegevens krijgt?▪ Verwijdert de leverancier/bewerker de persoonsgegevens enige tijd na beëindiging van de dienstverlening?
<input type="checkbox"/>	Adequate beveiligingsmaatregelen zijn noodzakelijk. Wordt de leverancier verplicht die te nemen? <ul style="list-style-type: none">▪ Zijn er specifieke normen of certificaten waaraan de leverancier/bewerker moet voldoen en zijn die benoemd?▪ Voor meer informatie zie de 'Richtsnoeren – Beveiliging van persoonsgegevens' die door het College bescherming persoonsgegevens zijn opgesteld.
<input type="checkbox"/>	Is afgesproken dat de school de beveiligingsmaatregelen mag controleren (of een audit mag laten voeren)? <ul style="list-style-type: none">▪ Is ook vastgelegd voor wie de kosten zijn?▪ Of laat de leverancier/bewerker zelf een onafhankelijke audit uitvoeren en levert hij daarvan een rapport/verklaring op?
<input type="checkbox"/>	Een softwareleverancier kan zaken uitbesteden aan subleveranciers, maar dat mag geen verschil maken voor de school. Dus: heeft de leverancier een (schriftelijke) overeenkomst gesloten waarin dezelfde verplichtingen zijn opgenomen als die voor hemzelf gelden? <ul style="list-style-type: none">▪ Zijn de subleveranciers ook verplicht tot geheimhouding en adequate beveiliging?▪ Mogen de subleveranciers ook alleen in opdracht van de school gegevens verwerken?

Waar moet u verder aan denken:

<input type="checkbox"/>	Let op of de gegevens alleen binnen Europa (Europese Economische Ruimte) worden opgeslagen en verwerkt. Wanneer een leverancier een vestiging in de Verenigde Staten heeft, ga dan na of deze leverancier gecertificeerd is onder de Amerikaanse Safe Harbour Principles. Zo niet, dan gelden namelijk aanvullende, vaak complexe regels.
<input type="checkbox"/>	Is de leverancier/bewerker contractueel verplicht om beveiligingsincidenten te melden? Is duidelijk dat de school (vooraf en tijdig) op de hoogte wordt gesteld? <ul style="list-style-type: none">▪ Wordt de leverancier verplicht om op eigen kosten alle benodigde maatregelen te nemen om gegevens veilig te stellen, tekortkomingen in beveiliging te herstellen en verder onbevoegde kennisneming, wijziging en verstrekking te voorkomen?▪ Zal de leverancier op verzoek van de school meewerken aan het informeren van de bevoegde autoriteiten en de leerlingen/ouders?
<input type="checkbox"/>	Backups van de gegevens zijn belangrijk. Zijn daar dingen over vastgelegd? Bijvoorbeeld over hoe vaak ze gemaakt worden? En over hoe snel of eenvoudig een backup teruggezet kan worden?
<input type="checkbox"/>	Is afgesproken dat de leverancier verplicht is om mee te werken aan verzoeken van leerlingen/ouders voor inzage/correctie/verwijdering van de persoonsgegevens? <ul style="list-style-type: none">▪ Als de leverancier daar een rechtstreeks verzoek voor krijgt, neemt die dan direct contact met de school op?▪ Wordt de school geïnformeerd als autoriteiten (zoals politie) om informatie vragen bij de leverancier?
<input type="checkbox"/>	Is er een boeteclausule als de leverancier/bewerker de afspraken niet nakomt? <ul style="list-style-type: none">▪ Is ook geregeld dat als de school aansprakelijk wordt gehouden voor een tekortkoming in de naleving van de bewerkersovereenkomst, dat verhaald kan worden op de leverancier?
<input type="checkbox"/>	Is afgesproken dat school en leverancier de Wet bescherming persoonsgegevens volledig en zorgvuldig nakomen?
<input type="checkbox"/>	Het is raadzaam op te nemen dat Nederlands recht van toepassing is op de overeenkomst en ook welke rechter bevoegd is. Is dat gebeurd? <ul style="list-style-type: none">▪ Zo niet: is duidelijk welk recht van toepassing is en welke rechters bevoegd zijn te oordelen over een geschil met de leverancier?

Aan de basis van deze checklist ligt de Wet bescherming persoonsgegevens. Het meeste gaat terug op de artikelen 10, 12, 13, 14, maar ook de artikelen 33, 34 en 76, 77 spelen mee. Daarnaast speelt de Wet meldplicht datalekken een rol. Raadpleeg bij twijfel over de toepassing van de checklist altijd de wet, of raadpleeg een privacy-deskundige.

Zie voor meer achtergronden en tips de website kennisnet.nl/privacy, de flyer "Privacy – Vuistregels voor omgaan met persoonsgegevens" en de algemene brochure 'Kinderen en online privacy'.

Deze checklist is een bewerking van de "Checklist privacy afspraken" van het SURFnet/Kennisnet Innovatieprogramma i.s.m. Project Moore Advocaten.



Stichting Kennisnet

Paletsingel 32
2718 NT Zoetermeer

Postbus 778
2700 AT Zoetermeer

T 0800 - 32 12 233
E info@kennisnet.nl
I kennisnet.nl