

Reader AVG voor personeelsleden



versie juni 2025

Disclaimer

Deze reader is met zorg samengesteld. Desondanks is het mogelijk dat de inhoud onvolledig en/of onjuist is. ICTotaal aanvaardt geen aansprakelijkheid voor eventuele fouten of onvolkomenheden. Raadpleeg in geval van twijfel de originele wetteksten en/of bronnen.

Reader voor personeelsleden – Inleiding

Waarom AVG?

De privacywet zorgt ervoor dat persoonsgegevens beter beschermd worden in een digitale wereld waarin steeds meer gegevens vastgelegd worden.

Grote bedrijven hebben een ongezonde honger naar data. Facebook en Google bijvoorbeeld weten al ontzettend veel van je en verdienen goed geld aan jouw gegevens. Maar ook scholen verwerken veel privacygevoelige informatie van leerlingen en hun verzorgers. Deze gegevens moeten zorgvuldig beschermd worden en mogen alleen onder strikte voorwaarden gedeeld worden met derden.

Privacy is een grondrecht

Privacy is het recht om met rust gelaten te worden.

Jouw personeelsdossier wordt zorgvuldig beschermd. Er is bepaald wie er toegang toe heeft (**grondslag**). Als personeelslid mag je precies weten welke gegevens de organisatie van jou heeft, wat ermee gedaan wordt, door wie ze mogen worden ingezien en hoe ze beschermd worden (**transparantie**). De organisatie mag niet meer gegevens over jou verzamelen dan strikt noodzakelijk (**data-minimalisatie**) en die gegevens mogen alleen gebruikt worden voor een van tevoren vastgesteld doel (**doelbinding**). Je mag de gegevens inzien en om correctie vragen wanneer zaken niet kloppen (**data-integriteit**).

Hetzelfde geldt natuurlijk ook voor leerlinggegevens. Het enige verschil is dat nu de ouders/ verzorgers degenen zijn die het recht hebben om het dossier van hun kind(eren) in te zien. De organisatie heeft de plicht om alle leerlingdata zorgvuldig te beschermen en ervoor te zorgen dat alleen direct betrokkenen (de groepsleerkrachten en de intern begeleider) er toegang toe hebben.

Onder de AVG moet een organisatie heel transparant zijn over welke gegevens er vastgelegd worden, wat er met die gegevens gebeurt en wie er toegang toe heeft.

Wat vraagt dit van mij als personeelslid?

Ga ervanuit dat ouders over je schouders meelezen wanneer je iets noteert over een leerling.

Zoals jij als leerkracht recht hebt om te weten wat er over jou wordt vastgelegd in het personeelsdossier, hebben de ouders (van minderjarige kinderen) het recht om (exact) te weten wat er in het leerlingdossier wordt vastgelegd. Dit vraagt om privacy volwassenheid van leerkrachten werkend in een professionele organisatie.

Wie doet wat?

Het omgaan met gegevens van anderen is een gezamenlijke verantwoordelijkheid van werkgever en werknemer.

Directeur-bestuurder:

aansprakelijke partij;

Privacy Officer:

Mirella Magnin,

(privacyteam@scholengroep Holland.nl)

centraal aanspreekpunt voor privacy zaken;

Directeur:

verantwoordelijk voor de uitvoering/handhaving van de AVG in de school;

ICT-coördinator:

regelt juiste toegang en juist gebruik van applicaties;

IB-er:

procesverantwoordelijk voor zorg data ParnasSys

Administratie:

(Geen administratie? Dan directeur verantwoordelijk)

procesverantwoordelijk voor de leerling administratie;

Personeelsleden:

aanspreekbaar op het correct omgaan met persoonsgegevens;

Functionaris Gegevensbescherming:

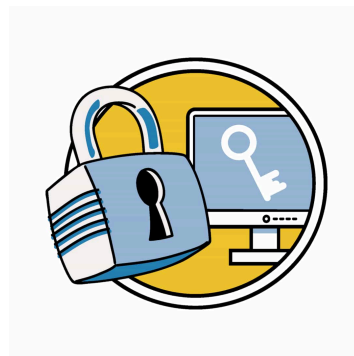
Rob van Son, (r.vanson@privaty.nl)

aanspreekpunt voor privacy vraagstukken voor personeelsleden, ouders, externen en de Autoriteit Persoonsgegevens; toezicht op naleving van de AVG.

Wachtwoorden zijn strikt persoonlijk

In verband met beveiliging én data-integriteit, zijn wachtwoorden strikt persoonlijk.

- Zorg dat je de enige bent die jouw wachtwoorden kent.
- Wijzig een wachtwoord wanneer een ander het zou kunnen weten.
- Wijzig belangrijke wachtwoorden minimaal 1x per jaar.
- Kies voor veilige, niet-voorspelbare wachtwoorden.



Wanneer je een ander laat werken onder jouw account, ben je – ook jaren later! – verantwoordelijk voor alles wat door die andere persoon onder jouw account heeft gedaan. Wanneer je gegevens van derden (kinderen) verwerkt kan je dat in (juridische) problemen brengen.

Voor scholen geldt:

- De invaller werkt onder het invalaccount of heeft een eigen account.

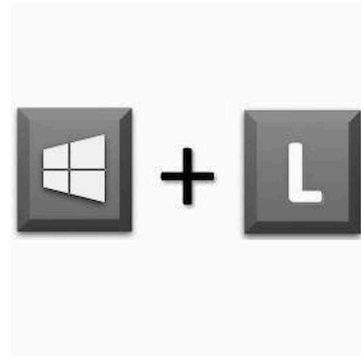
[Klik hier voor veel gestelde vragen over wachtwoorden](#)

Vergrendel je computer

Gebruik de toetsencombinatie Windows + L om je computer te vergrendelen.

Vergrendel je computer wanneer je je werkplek voor langere tijd verlaat – bijvoorbeeld in pauzes en tijdens gym.

- Hiermee voorkom je dat onbevoegden onder jouw gebruikersnaam in je mail kunnen snuffelen en documenten kunnen bekijken of veranderen. Dit is belangrijk omdat jij verantwoordelijk bent voor wat er onder jouw gebruikersnaam gebeurt.
- Het vergrendelen van je werkplek past bij een basale vorm van privacy bewustzijn.



Chromebook vergrendelen

- Op een chromebook is de toetsencombinatie **Launcher + L**.
(De launcher is de knop linksonder met het ronde symbool)

Berg de klassenmap op buiten schooltijd

Bewaar geen wachtwoorden en privacygevoelige informatie in de klassenmap.

Het best bewaarde geheim in onderwijsland: loop naar het bureau van de leerkracht en open de klassenmap. De kans is groot dat je daar (gevoelige) leerling gegevens én wachtwoorden vindt.

- Maak schoolafspraken over de vindplaats van de klassenmap.
- In de klassenmap worden geen privacy gevoelige gegevens bewaard.
- Maak schoolafspraken waar invaller gegevens kunnen opvragen als wachtwoorden, notities van leerlingen e.d.



📷 Voor foto's en video's is toestemming vereist

Foto's van kinderen mogen uitsluitend gepubliceerd worden na schriftelijke toestemming van ouders.

- Wanneer je op school foto's met je (privé)telefoon maakt, blijven de foto's op jouw toestel achter. Deze moet je na gebruik voor het vastgestelde doel verwijderen.
- In school mag een ouder alleen beeld- en geluidsopnamen maken als deze hiervoor toestemming heeft van de verantwoordelijke groepsleerkracht en/of de directie.
- Ouders mogen in school een (verjaardags)foto van hun kind maken voor eigen gebruik. Foto's waar anderen op staan, mogen door de ouder niet gedeeld worden op (bijvoorbeeld) sociale media.
- Voor het maken van foto's bij specifieke activiteiten moet specifieke toestemming geregeld worden. Denk bijvoorbeeld aan foto's van kamp, musical en afscheidsavond die je ook als aandenken wilt meegeven aan ouders.



[Klik hier voor veel gestelde vragen over foto's en filmmateriaal.](#)

🔗 Persoonsgegevens alleen delen (niet mailen!)

Het versturen van privacygevoelige informatie per e-mail kan alleen met aanvullende maatregelen! Standaard e-mail is onveilig!

Het probleem

Wanneer je een standaard mail verstuurt is dit te vergelijken met het versturen van een ansichtkaart of een brief in een open envelop.

Op het moment dat je de mail hebt verzonden ben je de controle kwijt. De mail zit nu als het ware in de rode brievenbus en legt nog een aantal stappen af voordat deze bij de ontvanger is:

- De rode brievenbus wordt geleegd
- De post gaat langs een paar sorteercentra
- De post wordt bezorgd bij de ontvanger

Op al deze plekken kan de post (automatisch) gelezen worden omdat de envelop niet is dichtgeplakt. Met de huidige stand van de techniek is het echter niet de vraag of dit gebeurt: ga er maar vanuit dát het gebeurt.

Wanneer de mail bij de ontvanger(s) is aangekomen, blijft deze mail (vaak nog jaren) in de mailbox aanwezig, zelfs wanneer de ontvanger de mail heeft weggegooid.

Stel dat er iets met de mailbox gebeurt... wie wordt er dan boos aangekeken op het feit dat jij bepaalde (vertrouwelijke) informatie hebt verstuurd?

Je voelt het al... dit moet veiliger en het kan veiliger!

Verstuur geen persoonsgegevens per mail. Hiervoor zijn veiligere alternatieven beschikbaar!

De oplossing

Met een aantal eenvoudige afspraken kun je mail een stuk veiliger maken:

- **Microsoft 365 mail:** Plak de envelop dicht met de optie **Versleutelen** in het bericht. Met deze simpele handeling voorkom je dat de mail onderweg gelezen kan worden.
Ook een eventueel meegestuurde bijlage is hiermee beveiligd.
- **Google mail:** Maak gebruik van de optie **Vertrouwelijke modus**. Hiermee kun je een e-mailbericht goed beveiligen.
- Stuur geen bijlage mee, maar deel deze met een link. Op deze wijze voorkom je dat de informatie ongevraagd en onbedoeld in de mailbox van de ontvanger achterblijft.
- Wanneer je de beschikking hebt over een e-maildienst als Zivver is dat dé manier om vertrouwelijke informatie mee te versturen.

- Via het ParnasSys ouderportaal kun je ouders toegang geven tot notities en handelingsplannen.
- Dossieruitwisseling verloopt via applicaties zoals OSO, Onderwijs Transparant, Groeidocumenten en Kindkans.

Algemene basisregels

- Gebruik de velden AAN: CC: en BCC op de juiste wijze
 - **AAN** = alleen de persoon die antwoord moet geven.
 - **CC** = de personen die mee mogen lezen, maar geen antwoord hoeven te geven.
 - **BCC** = hier plak je de adressen wanneer je een bericht naar een grote groep personen verstuurt, zodat ze elkaars e-mailadres niet kunnen zien.

E-mail is in de basis ongeschikt om privacygevoelige informatie mee te versturen. Maak gebruik van veiligere mogelijkheden.

Persoonsgegevens (bijv. een onderzoeksverslag) mogen alleen de organisatie verlaten wanneer daar een wettelijk geldige reden voor is, of expliciete toestemming (handtekening) van de betrokkene. **E-mail is in de basis ongeschikt** voor het versturen van **vertrouwelijke informatie**.

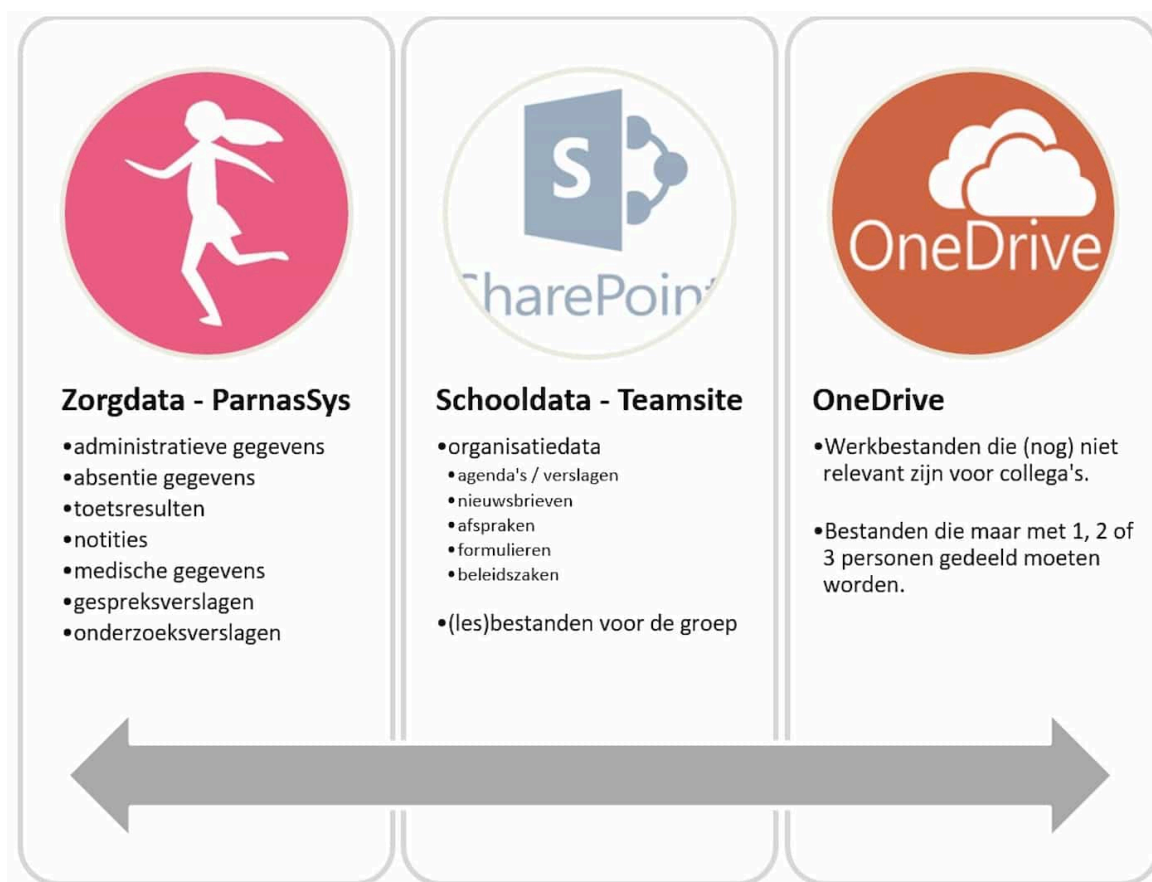


- Documenten met persoonsgegevens kun je indien nodig vanuit de Office werkomgeving DELEN met betrokkene.
- Bewaar geen persoonsgegevens in je mailbox!

Voor het mailen van vertrouwelijke gegevens maak je gebruik van **versleutelde mail** in Microsoft Office of **vertrouwelijkheid** in Google Workspace. Wanneer de organisatie gebruik maakt van Zivver, is dat dé manier privacygevoelige informatie te mailen.

Data alleen op goedgekeurde plaatsen

Gegevens over leerlingen moeten zorgvuldig beschermd worden en mogen daarom alleen op afgesproken plaatsen bestaan.



- Gegevens over leerlingen worden opgeslagen in ParnasSys, bij de betreffende leerling.
- Wanneer gegevens (nog) niet in ParnasSys kunnen staan, krijgen ze een plek binnen de Office werkomgeving (in de map 'zorg') of in de IB-map.
- In specifieke gevallen mogen bepaalde documenten met persoonsgegevens bestaan in je OneDrive.
- **USB-sticks zijn uitdrukkelijk verboden voor opslag van persoonsgegevens.**

In het schema hierboven kun je zien waar data van de organisatie hoort te staan.

Datalekken moeten gemeld worden

Een datalek moet binnen 72 uur gemeld zijn bij de Autoriteit Persoonsgegevens.

Wanneer gegevens onbedoeld in verkeerde handen terecht gekomen zouden kunnen zijn, **moet** dit gemeld worden. Het bewust niet melden van een (potentieel) datalek kan de organisatie flink in de problemen brengen.

- Datalekken komen voor, want mensen maken soms fouten.
- Het niet melden van een (potentieel) datalek kan leiden tot boetes, imagoschade en disciplinaire maatregelen.

Hoe meld je een (potentieel) datalek?

- Datalek melden kan bij de directie of via het **Meldpunt datalekken** <https://ibpmanager.nl/Meldpunt/rel/64337ad3-56b1-4e84-937e-4884ff776bb7/rid/4>.
- Je kunt ook een mail sturen naar privacyteam@scholengroep holland.nl.

Datalekken worden afgehandeld door de Functionaris Gegevensbescherming. Voor onze organisatie is dat:

Rob van Son – r.vanson@privaty.nl

Voorbeelden van (potentiële) datalekken

Houd je privé apparatuur veilig

Op je privé computer mogen vanzelfsprekend geen leerling gegevens staan.

- Sla documenten op in de Office werkomgeving (SharePoint / OneDrive).
- De instelling 'wachtwoord onthouden' van ParnasSys / de Office werkomgeving niet gebruiken wanneer huisgenoten op dezelfde computer werken.
- Vraag overzichten uit ParnasSys en andere onderwijsapplicaties alleen op op werkdevices.



- Leeg de map Downloads wanneer je overzichten uit ParnasSys hebt bekeken.

[Klik hier voor meer informatie over apparatuur in de thuisomgeving.](#)

Bijzondere persoonsgegevens zijn wettelijk extra beschermd

Voorbeelden van bijzondere persoonsgegevens zijn gegevens over gezondheid en levensbeschouwing (religie). Deze gegevens zijn wettelijk extra beschermd.

Persoonsgegevens zijn gegevens die betrekking hebben op een geïdentificeerde of identificeerbare natuurlijke persoon. Dit zijn alle gegevens die het leerlingvolgsysteem (ParnasSys), personeelsdossiers, groeidocumenten, Kindkans en Onderwijs Transparant worden opgeslagen. Ook foto's en video's vallen al snel onder bijzondere persoonsgegevens omdat er vaak veel informatie uit af te leiden is.



Voorbeelden van bijzondere persoonsgegevens zijn gegevens over gezondheid en levensbeschouwing (religie). Deze gegevens zijn wettelijk extra beschermd.

Voor scholen geldt:

- Medische gegevens uitsluitend opslaan in ParnasSys bij **medische gegevens**.

Voor uitwisseling met het samenwerkingsverband geldt:

- Maak gebruik van de afgesproken systemen (Kindkans, Grippa, Onderwijs Transparant) zodat vertrouwelijkheid gewaarborgd is.

Wanneer het voor de gezondheid noodzakelijk is dat informatie breder gedeeld moet worden (bijvoorbeeld een allergie of intolerantie) dan mag dit omdat daar dan een gerechtvaardigde reden voor is en omdat ouders hier toestemming voor geven.

Bijzondere persoonsgegevens mag je alleen opslaan en gebruiken onder bijzonder omstandigheden.

- Ras/etnische herkomst
- Politieke opvattingen
- Religieuze / levensbeschouwelijke opvattingen
- Lidmaatschap vakbond
- Genetische/biometrische gegevens
- Gezondheid
- Seksueel gedrag / gerichtheid
- Strafrechtelijke informatie

BSN (Burgerservicenummer) en religie mogen alleen worden gebruikt voor bij wet voorgeschreven doelen.

Wees transparant

Ouders hebben het recht om te weten welke gegevens over het kind worden opgeslagen en wie er toegang toe heeft.

Ouders hebben het recht om te weten welke gegevens de school over het kind heeft opgeslagen. De AVG biedt ze zelfs de mogelijkheid om een kopie van het dossier op te vragen.

- Noteer alleen feitelijke informatie in leerlingdossiers (ParnasSys).
- Houd jezelf scherp door bij alles wat je noteert te doen alsof ouders over je schouder met je meelesen. Dan kun je hierin eigenlijk geen fouten maken.
- Noteer niet meer dan noodzakelijk is voor het kunnen geven van goed onderwijs en voor de begeleiding van de leerling.



■ (Privé) telefoons en tablets

Een telefoon bevat veel informatie over jezelf en over anderen. Zorg dat het toestel goed beveiligd is.

Misschien vind je het prettig om e-mail van school op je eigen telefoon of tablet te ontvangen? Of je gebruikt de de Office werkomgeving, Parro- of andere app. Dit mag, maar vraagt wel om de volgende acties:

- Zorg dat je telefoon of tablet voorzien is van een pincode of beveiligingspatroon.
- Privételefoon verloren of gestolen? Dat is een datalek die je moet melden bij de organisatie.
- Heb je een bestand van de organisatie gedownload op je eigen tablet of telefoon? Verwijder dit dan direct na gebruik!



[Klik hier voor meer informatie over apparatuur in de thuisomgeving.](#)

👤 Gebruik alleen goedgekeurde leerlingprogramma's

Maak alleen gebruik programma's en websites die door de school/organisatie zijn goedgekeurd.

Als organisatie zijn we verantwoordelijk voor alle plaatsen waar we leerling gegevens opslaan. Dus ook die handige oefenwebsite, waar leerlingnamen ingevoerd moeten worden.

Voordat een nieuwe app, website of leerling programma in gebruik genomen wordt, moet hiervoor eerst een juridisch geldige overeenkomst worden afgesloten.



Functionaris Gegevensbescherming

Omdat een school veel persoonsgegevens van jonge (kwetsbare) kinderen verwerkt, moet de organisatie een Functionaris Gegevensbescherming hebben, die helpt om de privacyregels goed toe te passen.

Voor vragen kun je altijd contact opnemen via r.vanson@privaty.nl.

- Raadpleeg de FG voordat een nieuwe gegevensverwerking gaat plaatsvinden.
- Raadpleeg de FG voordat je met een nieuw leerlingprogramma wilt gaan werken.

Voor de organisatie is **Rob van Son** aangesteld als Functionaris Gegevensbescherming.

