

Privacy Beleid Stichting Penta

Vastgesteld door het bestuur: 9 januari 2019
Instemming GMR: 4 februari 2019

Kader privacy beleid

Februari 2019

Doel privacy beleid:

Het doel van het privacy beleid is het waarborgen van de bescherming van de persoonsgegevens van leerlingen en medewerkers die binnen Stichting Penta worden gebruikt. Het gaat hierbij niet alleen om gewone persoonsgegevens zoals naam, geboortedatum en overige contactgegevens, maar ook om bijzondere persoonsgegevens zoals bijvoorbeeld gegevens over de gezondheid.

Het schoolbestuur van Stichting Penta is verantwoordelijk voor de bescherming van de privacy van leerlingen en medewerkers en stelt dan ook het privacybeleid vast. Het privacybeleid is daarmee van toepassing op alle scholen die onder Stichting Penta vallen. Het privacybeleid is voorgelegd aan de Gemeenschappelijke Medezeggenschapsraad (GMR) en heeft van de GMR instemming verkregen.

Vanaf 25 mei 2018 is de Europese privacywet van toepassing: de Algemene Verordening Gegevensbescherming (AVG). De AVG formuleert een aantal belangrijke principes voor de verwerking van persoonsgegevens:

- Het gebruik van persoonsgegevens gebeurt op een wijze die rechtmatig, behoorlijk en transparant is;
- Het gebruik van die gegevens gebeurt alleen voor een uitdrukkelijk omschreven en gerechtvaardigd doel (doelbinding) en op een in de AVG genoemde grond (grondslag);
- Er worden niet meer persoonsgegevens gebruikt en vastgelegd dan strikt noodzakelijk is voor het doel waarvoor het wordt verwerkt (dataminimalisatie);
- Het gaat om juiste en geactualiseerde gegevens met redelijke maatregelen om waar nodig te rectificeren of te wissen (juistheid van de gegevens).

Binnen Stichting Penta hebben we op verschillende gebieden te maken met de AVG:

1. Privacybescherming leerling gegevens
2. Privacybescherming personeel
3. Privacybescherming personeel tijdens arbeidsverzuim

Deze bovengenoemde drie punten worden per onderdeel uitgewerkt. Per onderdeel wordt aangegeven wat nodig is voor de scholen en/of college van bestuur voor een goede uitvoering van het privacy beleid.

Privacybescherming leerling gegevens

Privacyreglement leerling gegevens

Alle scholen van Stichting Penta hanteren een gezamenlijk 'privacyreglement leerling gegevens' (bijlage 1), waarin allerlei zaken zijn vastgelegd omtrent de bescherming van de privacy.

Ouders hebben recht op inzage, correctie en het indienen van klachten aangaande de verwerking van persoonsgegevens van hun kind. Indien ouders hiervan gebruik willen maken, dienen zij hiervoor een schriftelijk verzoek in te dienen bij de schoolleider. Afhandeling van dit verzoek zal plaats vinden volgens de regels van het vastgestelde collectieve privacyreglement leerling gegevens.

Convenant Digitale Onderwijsmiddelen en Privacy 3.0

Digitale leermiddelen zijn niet meer weg te denken in het onderwijs. Het is belangrijk dat bij het gebruik van deze leermiddelen de privacy van leerlingen is beschermd. Hierbij hoort o.a. het maken van goede afspraken met aanbieders (educatieve uitgevers, distributeurs en leveranciers van leerling- en schooladministratiesystemen). Daarom hebben aanbieders van digitale leermiddelen en van andere digitale producten samen met de PO-raad en VO-raad afspraken gemaakt en dit vastgelegd in een convenant.

Dit 'Convenant Digitale Onderwijsmiddelen en Privacy 3.0' (bijlage 2) vertaalt onderdelen van de AVG naar de onderwijspraktijk.

Naast het maken van goede afspraken met aanbieders, regelt het convenant dat het college van bestuur alle ouders actief moet informeren hoe op iedere school wordt omgegaan met leerling gegevens. Stichting Penta geeft hierover uitleg op de website, middels het 'Privacyreglement verwerking leerling gegevens' (bijlage 1). De scholen geven uitleg op de website van de school en in de schoolgids hoe wordt omgegaan met leerling gegevens.

Model verwerkersovereenkomst 3.0

Bij dit convenant hoort een 'Model verwerkersovereenkomst 3.0' (bijlage 3). Hierin maakt de school met de leverancier afspraken over welke gegevens de leverancier mag gebruiken. In de overeenkomst staat ook welke beveiligingsmaatregelen de leverancier treft om de veiligheid van de verwerkte persoonsgegevens te waarborgen. Deze afspraken zijn juridisch afdwingbaar. Alle leveranciers die het convenant hebben ondertekend, zijn verplicht om deze model verwerkersovereenkomst te gebruiken. Scholen kunnen op de website van de PO-raad controleren of een leverancier het convenant heeft ondertekend (<https://www.privacyconvenant.nl/de-deelnemers>).

Reeds afgesloten Verwerkersovereenkomsten op basis van de modellen uit 2015 en 2016 blijven hun gelding houden totdat deze verwerkersovereenkomsten door partijen worden beëindigd.

In het model hoeven alleen de (contact)gegevens van de school en de leverancier te worden ingevuld. Voor de twee onderdelen c.q. bijlagen van de model verwerkersovereenkomst geldt het volgende:

1. In de Privacy bijsluiter (bijlage 1) wordt met name een beschrijving gegeven van de dienstverlening, producteigenschappen en welke categorieën Persoonsgegevens worden verwerkt en voor welke doeleinden.
2. In de Beveiligingsbijlage (bijlage 2) wordt omschreven welke technische en organisatorische beveiligingsmaatregelen er worden getroffen. De beveiliging dient een continue punt van aandacht en zorg te blijven.

Er hoeft per leverancier maar een verwerkersovereenkomst te worden gesloten, ook al worden er meer digitale producten geleverd. De verwerkersovereenkomst volgt de looptijd van het contract dat de school met de leverancier heeft afgesloten, bijvoorbeeld een licentie voor een schooljaar. Dus als er weer nieuwe contracten worden afgesloten met een leverancier, moeten er ook nieuwe verwerkersovereenkomsten worden getekend. Het is niet zo dat als een leverancier gebruik maakt van een eigen verwerkersovereenkomst deze daarom niet aan de eisen van wet- en regelgeving zou voldoen. Het is in dat geval wel aan de leverancier om gemotiveerd aan te geven waarom, en in hoeverre de eigen overeenkomst van de modelverwerkersovereenkomst afwijkt.

Het college van bestuur controleert periodiek of de benodigde verwerkersovereenkomsten aanwezig zijn. De controle frequentie wordt bepaald in overleg met de functionaris gegevensbescherming.

Meldplicht datalekken

Sinds 1 januari 2016 hebben alle scholen een meldplicht bij datalekken. Een datalek wordt door de school gemeld aan het college van bestuur. Het college van bestuur meldt het datalek bij de Autoriteit Persoonsgegevens via het webformulier dat op de website van de Autoriteit Persoonsgegevens beschikbaar is. De melding moet zonder onnodige vertraging en zo mogelijk niet later dan 72 uur na de ontdekking van het datalek worden gedaan. Zie voor meer informatie bijlage 4.

Sociale media

Sociale media worden steeds vaker door leerlingen en leraar gebruikt. De informatie die online wordt gedeeld, bevat vaak persoonsgegevens: een foto, naam, gedrag, uitnodiging of gesprek. Is het niet in de les, dan is het wel op het schoolplein. Internet en sociale media maken daarmee een onderdeel uit van het schoolklimaat. Om hierop in te kunnen spelen heeft iedere school een protocol sociale media.

Foto's en video's op school

Onder de Algemene Verordening Gegevensbescherming (AVG) heeft de school aantoonbaar toestemming nodig van ouders/verzorgers van leerlingen tot 16 jaar, voor het publiceren van beeldmateriaal van leerlingen. Dit is van toepassing op alle scholen binnen stichting Penta.

Bij geldige toestemming moet elke twijfel zijn uitgesloten en aan de volgende drie voorwaarden voldoen:

1. De toestemming moet vrij en niet onder druk gegeven zijn. De ouder mag bijvoorbeeld niet benadeeld worden als hij of zij geen toestemming geeft.
2. De toestemming moet ondubbelzinnig zijn. Het moet dus volstrekt helder zijn dat er toestemming is verleend. Er mag niet uitgaan worden van het principe 'wie zwijgt, stemt toe'.
3. Er wordt toestemming gevraagd voor een specifieke verwerking en een specifiek doel. Bijvoorbeeld om via foto's en video's op uw website verslag te doen van een schoolreisje aan alle ouders.

Daarnaast moet het voor ouders net zo makkelijk zijn om de toestemming weer in te trekken als om de toestemming te geven.

De school hoeft niet elk jaar opnieuw toestemming te vragen, maar kan de toestemming bijvoorbeeld bij de inschrijving van de leerling regelen. Bij wijzigingen of aanpassingen van de verwerking moet de school opnieuw om toestemming vragen. De school kan er daarnaast voor kiezen om de ouders periodiek te informeren over de vraag waarvoor zij precies eerder toestemming hebben gegeven.

Informatieve sites over privacy op school:

De Autoriteit Persoonsgegevens (AP) heeft een onderdeel van hun site specifiek gewijd aan scholen:

<https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/onderwijs/scholen-de-avg>

Op de site www.kennisnet.nl is onder andere te vinden:

- Voorbeeldteksten over privacy in bijv. schoolgids en website
- Modelreglement internet en sociale media
- Voorbeeldbrief voor toestemming gebruik foto's en video's

Zie hiervoor deze link: <https://www.kennisnet.nl/artikel/alle-privacyhulpmiddelen-voor-scholen-op-een-rij/>

Privacybescherming personeel

Alle scholen van Stichting Penta hanteren een gezamenlijk 'privacyreglement personeelsgegevens' (bijlage 6) waarin allerlei zaken zijn vastgelegd omtrent de bescherming van de privacy. In grote lijnen worden achtereenvolgens de reikwijdte en doelstelling van dit reglement genoemd, het beheer en de verwerking van gegevens en de doelstelling daarvan, de gegevensverstrekking en andere rechten en plichten zoals het recht op inzage, de informatieplicht e.d. Tevens bevat het privacyreglement een overzicht van diegenen die toegang hebben tot de personeelsregistratie van Stichting Penta.

Naast het 'privacyreglement personeelsgegevens' hanteert Stichting Penta een Elektronische Informatie- en Communicatiemiddelen (EIC)-regeling (zie bijlage 7). In deze regeling wordt aangegeven op welke wijze wordt omgegaan met elektronische informatie- en communicatiemiddelen binnen onze stichting.

Privacybescherming personeel tijdens arbeidsverzuim

De Autoriteit Persoonsgegevens (AP) heeft in april 2016 een publicatie uitgebracht: 'De zieke werknemer' Beleidsregels voor de verwerking van persoonsgegevens over de gezondheid van zieke werknemers. De AP zal streng blijven toezien op de verwerking van gevoelige medische gegevens en het gebruik van persoonsgegevens binnen de arbeidsrelatie. Zie hiervoor deze link: <https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/werk-en-uitkering/zieke-werknemers?qa=de%20zieke%20werknemer&scrollto=1>

In de praktijk mag de werkgever bij een ziekmelding het volgende vragen en registreren:

- Het telefoonnummer en (verpleeg)adres;
- De vermoedelijke duur van het verzuim;
- De lopende afspraken van werkzaamheden;
- Of de werknemer onder een van de vangnetbepalingen van de Ziektewet valt (maar niet onder welke bepaling hij/zij valt);

- Of de ziekte verband houdt met een arbeidsongeval;
- Of er sprake is van een verkeersongeval waarbij een eventueel aansprakelijke derde betrokken is (regresmogelijkheid).

De werkgever mag in principe geen andere gegevens over de gezondheid verwerken dan de hierboven genoemde gegevens. Ook niet met toestemming van de werknemer. Gelet op de gezagsverhouding tussen werkgever en werknemer kan een werknemer zich immers gedwongen voelen toestemming te verlenen. Alleen wanneer een werknemer een ziekte heeft waarbij het noodzakelijk kan zijn dat directe collega's in geval van nood weten hoe te handelen (bijv. bij epilepsie of suikerziekte), mag de werkgever de vrijwillig door de werknemer verstrekte gegevens over zijn ziekte registreren.

Welke gegevens mag de werkgever verwerken?

Naast de gegevens van de ziekmelding mag de werkgever gegevens verwerken die de bedrijfsarts aan hem heeft verstrekt over:

- De werkzaamheden waartoe de werknemer niet meer of nog wel in staat is (functionele beperkingen, restmogelijkheden en implicaties voor het soort werk dat de werknemer nog kan doen;
- De verwachte duur van het verzuim;
- De mate waarin de werknemer arbeidsongeschikt is (gebaseerd op de functionele beperkingen, restmogelijkheden en implicaties voor het soort werk dat de werknemer nog kan doen);
- Eventuele adviezen over aanpassingen, werkvoorzieningen of interventies die de werkgever voor de re-integratie moet treffen.

Plan van aanpak

Uiterlijk twee weken na het advies van de bedrijfsarts, dus uiterlijk in de achtste week van het verzuim, moeten de werkgever en de werknemer gezamenlijk een plan van aanpak opstellen. In het plan van aanpak mogen alleen die gegevens over de gezondheid opgeschreven worden die voor het opstellen van het plan van aanpak noodzakelijk zijn, zoals de door de bedrijfsarts vastgestelde beperkingen en mogelijkheden van de werknemer en wat deze betekenen voor het soort werk dat hij/zij kan doen.

Dus geen gegevens over aard en oorzaak van de ziekte.

In bijlage 8 hebben wij de beleidsregels zoals de AP deze stelt (uitgebreid) op een rijtje gezet.

N.B.: De door de Autoriteit Persoonsgegevens (AP) in april 2016 uitgebrachte publicatie: 'De zieke werknemer' Beleidsregels voor de verwerking van persoonsgegevens over de gezondheid van zieke werknemers, is op basis van de (oude) Wet bescherming persoonsgegevens (Wbp) opgesteld. Er is nog geen nieuwe versie op basis van de AVG beschikbaar.