**PRIVACYREGLEMENT**

**Medewerkers**

Versie 0.2
Auteur: Niels Dutij – Peter Vermeijs

Inhoud

[Inleiding 3](#_Toc514397662)

[1. Algemene bepalingen 4](#_Toc514397663)

[1. Definitie belangrijkste begrippen 4](#_Toc514397664)

[2. Reikwijdte en doelstelling privacyreglement 5](#_Toc514397665)

[3. Inwerkingtreding en duur privacyreglement 5](#_Toc514397666)

[4. Reikwijdte privacyreglement 5](#_Toc514397667)

[5. Doel privacyreglement 5](#_Toc514397668)

[6. Aanspreekbaarheid 5](#_Toc514397669)

[2. Verplichtingen van de Onderwijsinstelling 6](#_Toc514397670)

[1. Professioneel en integer handelen 6](#_Toc514397671)

[2. Informeren van medewerkers 6](#_Toc514397672)

[3. Functionaris voor de gegevensbescherming 6](#_Toc514397673)

[4. DPIA 6](#_Toc514397674)

[5. Beveiliging en geheimhouding 7](#_Toc514397675)

[6 Datalekken 7](#_Toc514397676)

[3. Persoonsgegevens 8](#_Toc514397677)

[1 Doel en verwerking van de persoonsgegevens 8](#_Toc514397678)

[2. Wijze van verkrijgen van persoonsgegevens 8](#_Toc514397679)

[3. Aanmelden op ICT voorzieningen van de Onderwijsinstelling 8](#_Toc514397680)

[4. Monitoring 9](#_Toc514397681)

[4. Het verwerken van persoonsgegevens 10](#_Toc514397682)

[1. Verwerken van persoonsgegevens 10](#_Toc514397683)

[2. Toegang tot de persoonsregistratie en beveiliging 10](#_Toc514397684)

[3. Bewaren en verwijderen van opgenomen gegevens 10](#_Toc514397685)

[4. Bewaartermijnen 11](#_Toc514397686)

[5. Richtlijnen verstrekking van persoonsgegevens 12](#_Toc514397687)

[1. Grondslag voor verstrekking persoonsgegevens aan derden 12](#_Toc514397688)

[2. Juridische toetsing van verzoeken 12](#_Toc514397689)

[3. Schriftelijke afspraken over gegevensverstrekking 12](#_Toc514397690)

[6. Uitvoering rechten van medewerkers 14](#_Toc514397691)

[1. Inzage persoonsgegevens 14](#_Toc514397692)

[2. Correctie persoonsgegevens 14](#_Toc514397693)

[3. Schending recht 15](#_Toc514397694)

[4. Klachten 15](#_Toc514397695)

# Inleiding

Wij bieden onze medewerkers een veilige werkplek. Een goede en zorgvuldige omgang met persoonsgegevens binnen de school is daarvoor een randvoorwaarde.

De Algemene Verordening Gegevensbescherming (AVG) stelt nieuwe en verdergaande eisen aan de omgang met persoonsgegevens. Het privacyreglement van [naam stichting/vereniging] en het beleid dat daaraan ten grondslag ligt hebben wij daarom herzien en aangevuld op de punten waar de AVG dit vereist.

Met het reglement beoogt …- naam school- .. zorg te dragen dat de verwerking van persoonsgegevens plaatsvindt conform de Verordening, de implementatiewet Verordening, sectorgedragscodes, sectorbeveiligingscodes en organisatie-specifieke (interne) regelingen.

Dit houdt onder andere in dat:

* + - 1. de persoonlijke levenssfeer van medewerkers wordt beschermd tegen onrechtmatige verwerking en/of misbruik van die gegevens, tegen verlies en tegen het verwerken van onjuiste gegevens;
			2. wordt voorkomen dat persoonsgegevens worden verwerkt voor een ander doel dan het doel waarvoor ze verzameld zijn; en
			3. de verwerkingen niet leiden tot een hoog risico voor de medewerkers.

Het college van bestuur zal in samenspraak met de functionaris gegevensbescherming passende maatregelen ten uitvoer leggen en verantwoording afleggen over het gevoerde beleid aan de

betreffende medezeggenschapsorganen en aan de Raad van Toezicht.

College van bestuur

# Algemene bepalingen

## 1. Definitie belangrijkste begrippen

In dit reglement wordt verstaan onder:

*Bijzondere persoonsgegevens:* Een persoonsgegevens dat iets zegt over iemand zijn godsdienst, levensovertuiging, ras, politieke gezindheid en gezondheid;

*Derde:* Iedereen die niet bij de verwerking betrokken is zoals het ABP, de accountant etc

*De Onderwijsinstelling;* Een of meerdere onderdelen van ….naam school…,

*Minderjarigen:* De student die de leeftijd van 16 jaar nog niet heeft bereikt;

*Ouder(s):* De wettelijk vertegenwoordiger van de student;

*Persoonsgegevens:* Alle informatie over een natuurlijke persoon (mens van vlees en bloed) zoals naam, leeftijd, geslacht etc. Hieronder vallen ook ‘digitale’ persoonsgegevens, zoals ip-adressen, locatiegegevens, de websites die je bezoekt etc.

*Data Protection impact assessment:* Instrument om vooraf de privacyrisico’s van een verwerking in kaart te brengen om vervolgens maatregelen te nemen om de risico’s te verkleinen;

*Privacy:* Privacy wordt in de Nederlandse grondwet ‘eerbiediging van de persoonlijke levenssfeer’ genoemd;

*Monitoring:* Monitoring is het bewaken van gegevens van de logging met betrekking tot de ICT voorzieningen;

*Medewerker;* De betrokkene in de zin van de wet over wie de persoonsgegevens iets zeggen, in dit reglement spreken we altijd over personen die een dienstverband hebben met de Onderwijsinstelling of (mogelijk) werkzaamheden verrichten voor de Onderwijsinstelling.

*Toestemming:* Ondubbelzinnige wilsuiting waarmee de student door middel van een verklaring of een ondubbelzinnige actieve handeling verwerking van persoonsgegevens aanvaard;

*Toezichthoudende autoriteit:* De Autoriteit Persoonsgegevens;

*Verwerker:* Een bedrijf, organisatie of leverancier die in opdracht van de Onderwijsinstelling de persoonsgegevens verwerkt;

*Verwerkingsverantwoordelijke:* De Onderwijsinstelling (de verantwoordelijke onderwijsinstelling / het bevoegd gezag);

*Verwerking van persoonsgegevens:* Alles wat met persoonsgegevens gedaan wordt, zoals het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, doorsturen etc.

## 2. Reikwijdte en doelstelling privacyreglement

1. Dit privacyreglement wordt na instemming van de Ondernemingsraad vastgesteld, op de op de voorpagina genoemde datum, door het bevoegd gezag.

2. Dit privacyreglement vervangt alle eerdere privacyreglementen van de Onderwijsinstelling.

3. In situaties waarin dit privacyreglement geen uitsluitsel verschaft, beslist het College van Bestuur.

## 3. Inwerkingtreding en duur privacyreglement

1. Het privacyreglement kan tussentijds worden gewijzigd op verzoek van het College van Bestuur.

2. Indien partijen geen verzoek tot wijziging van het privacyreglement aan de ander hebben kenbaar gemaakt, wordt het privacyreglement van rechtswege verlengd voor onbepaalde tijd.

## 4. Reikwijdte privacyreglement

1. Dit privacyreglement gaat over het gebruik van persoonsgegevens van medewerkers, sollicitanten en andere personen die op basis van andersoortige contracten werkzaam zijn voor de Onderwijsinstelling..

2. In dit privacyreglement wil de Onderwijsinstelling met een aantal regels openheid bieden aan medewerkers over hoe de Onderwijsinstelling omgaat met de aan haar toevertrouwde gegevens.

3. Dit privacyreglement is niet van toepassing op persoonsgegevens opgenomen in bestanden van de Vertrouwenspersoon, de Ombudsman en / of de Klachten- en Geschillencommissies. De vertrouwelijkheid van deze gegevens is geregeld in desbetreffende regelingen en / of de cao.

## 5. Doel privacyreglement

1. Dit privacyreglement wenst:

 a. de privacy van de medewerker te beschermen tegen verkeerd en onbedoeld gebruik van persoonsgegevens;

 b. toe te lichten welke persoonsgegevens worden verwerkt en met welk doel dit gebeurt;

 c. de zorgvuldige verwerking van persoonsgegevens te waarborgen en

 d. de rechten van de medewerker te waarborgen.

## 6. Aanspreekbaarheid

1. De Onderwijsinstelling en de specifieke medewerkers die de gegevens verwerken en beheren worden geacht de inhoud van het privacyreglement te kennen en zich hieraan te houden.

2. Medewerkers van de Onderwijsinstelling zijn te allen tijde aanspreekbaar op het naleven van het privacyreglement.

3. Het privacyreglement is gepubliceerd op de website van de Onderwijstelling.

# 2. Verplichtingen van de Onderwijsinstelling

## 1. Professioneel en integer handelen

1. De Onderwijsinstelling gaat op een zorgvuldige, veilige en vertrouwelijke manier met de persoonsgegevens om. Deze verplichting vervalt voor informatie die op basis van wettelijke verplichtingen moet worden aangeleverd.

2. De Onderwijsinstelling spant zich in om:

* de persoonlijke levenssfeer van de student te beschermen tegen verlies of misbruik van de gegevens en opslag van onjuiste gegevens;
* te voorkomen dat gegevens voor een ander doel worden gebruikt dan waarvoor deze zijn verstrekt;
* de rechten van de medewerker te waarborgen.

## 2. Informeren van medewerkers

1. De Onderwijsinstelling is verplicht om de onderstaande informatie aan de medewerker te verstrekken:

* de identiteit van de onderwijsinstelling;
* de doeleinden van de verwerking;
* de contactgegevens van de vertegenwoordiger van de Onderwijsinstelling;
* de contactgegevens van de functionaris gegevensbescherming;
* de ontvangers van persoonsgegevens;
* het bestaan van de rechten van medewerkers;
* de bewaartermijnen van de persoonsgegevens;
* het recht om een klacht in te dienen bij de Autoriteit Persoonsgegevens;
* nadere informatie voor zover dat nodig is om een zorgvuldige verwerking te waarborgen.

## 3. Functionaris voor de gegevensbescherming

1. De Onderwijsinstelling heeft een Functionaris voor de gegevensbescherming aangesteld.

2. De Functionaris voor de gegevensbescherming vervult ten minste de onderstaande taken:

* toezicht houden op de naleving van wet- en regelgeving, alsmede naleving van het privacyreglement;
* fungeren als centraal meldpunt voor vragen en klachten over het privacybeleid.

## 4. DPIA

1. In de onderstaande gevallen is het uitvoeren van een data protection impact assessment (hierna: DPIA) verplicht:

* bij het instellen van een systematische en uitvoerige evaluatie van persoonlijke aspecten, waaronder profilering;
* op grote schaal het verwerken van bijzondere persoonsgegevens;
* op grote schaal en systematisch het volgen van mensen in een publiek toegankelijk gebied (bijv. cameratoezicht).
1. De Onderwijsinstelling verwerkt op grote schaal persoonsgegevens van medewerkers. De Onderwijsinstelling is dan ook verplicht om periodiek een DPIA uit te voeren.

## 5. Beveiliging en geheimhouding

1. De Onderwijsinstelling draagt zorg voor passende technische en organisatorische maatregelen ter voorkoming van verlies of onrechtmatige verwerking van persoonsgegevens. Deze maatregelen garanderen, rekening houdend met de stand der techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau, gelet op de risico’s die de verwerking en de aard van de te beschermen gegevens met zich meebrengen. De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen.
2. Een ieder die betrokken is bij de uitvoering van dit reglement en daarbij de beschikking krijgt over persoonsgegevens waarvan hij het vertrouwelijke karakter kent of redelijkerwijs kan vermoeden en voor wie niet reeds uit hoofde van beroep, functie of wettelijk voorschrift ter zake van de persoonsgegevens een geheimhoudingsplicht geldt, is verplicht tot geheimhouding daarvan. Dit geldt niet indien enig wettelijk voorschrift hem tot bekendmaking verplicht of uit zijn taak bij de uitvoering van dit reglement de noodzaak tot bekendmaking voortvloeit.

## 6 Datalekken

1. Indien binnen de Onderwijsinstelling zelf of bij een door de Onderwijsinstelling ingeschakelde verwerker een inbreuk op de beveiliging voordoet, waarbij een aanzienlijke kans bestaat op verlies of onrechtmatige verwerking van persoonsgegevens die door de Onderwijsinstelling worden verwerkt, dan wel dit verlies of onrechtmatige verwerking zich daadwerkelijk voordoet, zal de Onderwijsinstelling daarvan melding doen bij de Autoriteit Persoonsgegevens, tenzij kan worden aangetoond dat het onwaarschijnlijk is dat deze inbreuk risico’s voor de rechten en vrijheden van natuurlijke personen met zich brengt.
2. De Onderwijsinstelling zal iedere inbreuk op de beveiliging documenteren, ongeacht of deze wordt gemeld bij de Autoriteit Persoonsgegevens.
3. Indien de inbreuk een hoog risico voor de rechten en vrijheden van de medewerker inhoudt, stelt de Onderwijsinstelling ook de medewerker onverwijld in kennis van de inbreuk. Deze mededeling kan achterwege blijven indien:
* de persoonsgegevens versleuteld zijn en niet toegankelijk voor derden;
* er inmiddels maatregelen getroffen zijn die het hoge risico hebben weggenomen;
* de mededeling een onevenredige inspanning vergt. Een openbare mededeling kan dan volstaan.
1. Bij het vaststellen of sprake is van een inbreuk op de beveiliging en of melding daarvan moet

worden gedaan bij de Autoriteit Persoonsgegevens hanteert de Onderwijsinstelling de procedures die zijn opgenomen in beleid en protocol Datalekken.

# 3. Persoonsgegevens

## 1 Doel en verwerking van de persoonsgegevens

1. De Onderwijsinstelling streeft bij het verwerken van gegevens naar een minimalistische vastlegging (zo min mogelijk) van persoonsgegevens. Dit houdt in dat alleen gegevens worden verwerkt die benodigd zijn voor het uitvoeren van de overeenkomst en de daarbij komende verplichtingen.
2. De verwerking van de gegevens moet in overeenstemming zijn met het doel, waarvoor zij zijn verkregen. De doeleinden verschillen per categorie en zijn inzichtelijk in het opgestelde dataregister.
3. De categorieën van persoonsgegevens zijn:
	1. Contactgegevens beperkt (naam, e-mail adres en organisatorische eenheid)
	2. Contactgegevens volledig
	3. Personeelsnummer
	4. Nationaliteit en geboorteplaats
	5. Medische gegevens (op eigen verzoek)
	6. Ervaringen (werkervaringen en opleidingen)
	7. RenO gesprekken (Resultaat en ontwikkeling)
	8. Financiën (inclusief de financiële cyclus)
	9. Beeldmateriaal
	10. Overige gegevens
	11. BSN

## 2. Wijze van verkrijgen van persoonsgegevens

1. De persoonsgegevens worden voor zover mogelijk door de medewerker zelf bij de indiensttreding.

2. De persoonsgegevens worden door de daartoe bevoegde en geautoriseerde medewerkers in het personeelsdossier gezet en onderhouden.

4. Indien de Onderwijsinstelling extra informatie nodig heeft over de medewerkers, zal zij deze uitsluitend opvragen als de Onderwijsinstelling daarvoor een wettelijke grondslag heeft.

## 3. Aanmelden op ICT voorzieningen van de Onderwijsinstelling

1. Een ieder die gebruik wil maken van onze ICT voorzieningen (bijvoorbeeld WIFI) moet zich aanmelden met een persoonlijk inlogaccount.

2. Vanuit het Informatie Beveiligingsbeleid en de SURFnet voorwaarden wordt gesteld dat er niet anoniem gebruik gemaakt kan worden van de ICT voorzieningen en de internet verbinding van de Onderwijsinstelling. Dat betekent dat men zich altijd moet aanmelden voordat gebruik kan worden gemaakt van een ICT voorziening (Computer, Telefoon, Wireless, Portaal voor Talent, etc).

3. In het reglement verantwoord gebruik ICT-faciliteiten voor medewerkers legt de Onderwijsinstelling vast wat de randvoorwaarden zijn.

4. Elk medewerker wordt geacht de inhoud van het reglement verantwoord gebruik ICT-faciliteiten voor medewerkers te kennen en zich hieraan te houden.

5. Het reglement verantwoord gebruik ICT-faciliteiten voor medewerkers is door de medewerker in te zien op de website van de Onderwijsinstelling.

## 4. Monitoring

1. Aanmelden op de ICT voorziening houdt automatisch in dat er getraceerd en gemonitord kan en zal worden. Dit is noodzakelijk voor het zo stabiel mogelijk draaien van WIFI en voor het zo snel mogelijk kunnen traceren van ongeregeldheden.

2. Ten behoeve van optimale ICT voorzieningen maakt de Onderwijsinstelling gebruik van monitoring tools en logging. De monitoring tools en logging worden enkel en alleen gebruikt voor ICT beheer optimalisatie en / of voorkomen of oplossen van ongeregeldheden binnen ons netwerk.

3. Voor meer informatie over de ICT voorziening kan de medewerker het reglement verantwoord gebruik ICT-faciliteiten voor medewerkers raadplegen.

# 4. Het verwerken van persoonsgegevens

## 1. Verwerken van persoonsgegevens

1. Bij de verwerking van persoonsgegevens houdt de Onderwijsinstelling zich aan de wet.

2. De verwerking van persoonsgegevens vindt plaats onder meer door (maar niet beperkt tot):

A. Uitvoering van de overeenkomst

* Komen tot een aanstelling (overeenkomst)
* Overeenkomsten met externe bewerkers (ADP, QMP, Office365, etc.

B. Wettelijke plicht:

* Voldoen aan de wettelijke verplichtingen (Belasting, pensioen, etc.)

C. Gerechtvaardigd belang:

* het uitvoeren van videocameratoezicht.

## 2. Toegang tot de persoonsregistratie en beveiliging

1. De Onderwijsinstelling zorgt ervoor dat de toegang tot de administratie en systemen beperkt is. Medewerkers van de Onderwijsinstelling hebben slechts toegang tot de verwerkingen van persoonsgegevens als dat noodzakelijk is voor de uitvoering van hun functie.

2. Iedereen die binnen de Onderwijsinstelling persoonsgegevens verwerkt, is verplicht daar vertrouwelijk mee om te gaan.

3. De verwerker en derden van de Onderwijsinstelling staan hebben toegang tot de persoonsregistratie indien;

* de verwerker gemachtigd is om persoonsgegevens te verwerken;
* een derde die op grond van een wet toegang moet worden verleend of de Onderwijsinstelling een gerechtvaardigd belang heeft.

4. De Onderwijsinstelling is verantwoordelijk voor de naleving van de bepalingen uit dit reglement en voor de juistheid en de volledigheid van de opgenomen gegevens.

5. De Onderwijsinstelling draagt zorg voor de nodige voorzieningen van fysieke, technische en organisatorische aard ter beveiliging van de persoonsregistraties tegen verlies of onrechtmatige verwerking van de gegevens en tegen onbevoegde kennisneming.

## 3. Bewaren en verwijderen van opgenomen gegevens

1. De gegevens mogen niet langer worden bewaard dan noodzakelijk.

2. De Onderwijsinstelling houdt zich aan de wettelijke vernietigings- en bewaartermijnen.

3. Vernietiging blijft evenwel achterwege wanneer:

1. redelijkerwijs aannemelijk is dat de bewaring van aanmerkelijk belang is voor een ander dan de medewerker;
2. de zorg van een goede administratie of rechtszaak bewaring noodzaakt;
3. bewaring op grond van een wettelijk voorschrift vereist is;
4. indien daarover tussen de student en de Onderwijsinstelling overeenstemming bestaat.
5. Indien de betreffende gegevens zodanig zijn bewerkt, dat herleiding tot individuele personen redelijkerwijs onmogelijk is, kunnen zij in geanonimiseerde vorm bewaard blijven.

## 4. Bewaartermijnen

1. De gegevens mogen niet langer worden bewaard dan noodzakelijk, tenzij er een wettelijk verplicht gestelde bewaartermijn geldt. Hierbij onderscheiden we:
2. Administratie personeel / salaris: de persoonsgegevens worden verwijderd uiterlijk twee jaren nadat het dienstverband of de werkzaamheden van medewerker ten behoeve van de Onderwijsinstelling zijn beëindigd, tenzij de persoonsgegevens noodzakelijk zijn ter voldoening aan een wettelijke bewaarplicht.
3. Administratie sollicitanten: de persoonsgegevens worden verwijderd op een daartoe strekkend verzoek van betrokkene en in ieder geval uiterlijk vier weken nadat de sollicitatieprocedure is geëindigd, tenzij de persoonsgegevens met schriftelijke toestemming van betrokkene gedurende een jaar na beëindiging van de sollicitatieprocedure worden bewaard.

# 5. Richtlijnen verstrekking van persoonsgegevens

## 1. Grondslag voor verstrekking persoonsgegevens aan derden

1. Het verstrekken van gegevens aan derden kan in ieder geval geschieden op basis van:

 A.Uitvoering wettelijke plicht

 De Onderwijsinstelling is gebonden aan wetgeving, deze maakt het noodzakelijk om in bepaalde situaties persoonsgegevens van medewerkers aan externe partijen te verstrekken.

B.Gerechtvaardigd belang

1. De Onderwijsinstelling zal persoonsgegevens mogen verwerken en uitwisselen voor zover noodzakelijk is voor de behartiging van een gerechtvaardigd belang van haarzelf of dat van een derde aan wie de gegevens worden verstrekt, tenzij het belang of de fundamentele rechten en vrijheden van de medewerker prevaleert. Dat gerechtvaardigd belang dient aantoonbaar te prevaleren boven de belangen van de medewerkers..

2. Op grond van gerechtvaardigd belang kunnen onder meer persoonsgegevens aan derden verstrekt worden voor zover dit noodzakelijk is:

* voor het in handen van derden stellen van vorderingen;
* voor het behandelen van geschillen;
* voor het doen verrichten van accountantscontroles.

C. Toestemming van de medewerker

1. Mocht er geen andere wettelijke grondslag voor gegevensuitwisseling kunnen worden aangetoond door de derde, dan zal de verstrekking van persoonsgegevens alleen mogen gedaan met de toestemming van de medewerker.

2. De Onderwijsinstelling verschaft informatie over de gegevensuitwisseling aan de medewerker.

## 2. Juridische toetsing van verzoeken

1. Voor de toetsing van verzoeken om persoonsgegevens heeft de Onderwijsinstelling onderstaande richtlijnen opgesteld.

2. Elk verstrekking van persoonsgegevens moet naast een grondslag voldoen aan de volgende eisen:

* Subsidiariteit
* Proportionaliteit
* Dataminimalisatie

Subsidiariteit

Het doel waarvoor de persoonsgegevens worden verwerkt kan in redelijkheid niet op een andere, voor de bij medewerker minder nadelige wijze worden verwerkelijkt.

Proportionaliteit

De inbreuk op de belangen van de medewerker, mag niet onevenredig groot zijn in verhouding tot het met de verwerking te dienen doel.

 Dataminimalisatie

De Onderwijsinstelling zal niet langer en ook niet **meer** gegevens verstrekken dan noodzakelijk is voor het dienen van het belang van de derde. De Onderwijsinstelling zal dan ook niet de volledige administratie verstrekken, maar alleen dat gedeelte waarmee de derde haar doel kan bereiken.

## 3. Schriftelijke afspraken over gegevensverstrekking

1. Wanneer de Onderwijsinstelling persoonsgegevens al dan niet op regelmatige basis, aan een derde verstrekt, maken partijen hierover schriftelijke afspraken.

2. Wanneer de Onderwijsinstelling een derde inschakelt die de persoonsgegevens namens haar verwerkt, moet daarmee een verwerkersovereenkomst worden afgesloten.

# 6. Uitvoering rechten van medewerkers

## 1. Inzage persoonsgegevens

A Recht van inzage

1. De medewerker heeft het recht te weten of / en welke persoonsgegevens worden verwerkt door de Onderwijsinstelling. De Onderwijsinstelling moet de medewerker zo spoedig mogelijk, doch uiterlijk binnen vier weken na ontvangst van het verzoek tot inzage, een kopie verstrekken van de persoonsgegevens die worden verwerkt. Aan een verzoek om bijkomende kopieën kunnen kosten worden verbonden.

2. Voordat een medewerker inzage krijgt in zijn dossier dient de medewerker zich te legitimeren. De Onderwijsinstelling zal geen kopie van het identiteitsbewijs in de administratie opnemen bij het vaststellen van de identiteit.

3. De Onderwijsinstelling draagt steeds zorg voor een deugdelijke vaststelling van de identiteit van de medewerker.

## 2. Correctie persoonsgegevens

B. Recht op rectificatie

1. De medewerker heeft recht op verbetering, aanvulling of verwijdering van op hem betrekking hebbende persoonsgegevens, onder meer door een aanvullende verklaring te verstrekken. De rectificatie moet meteen plaatsvinden.

2. De Onderwijsinstelling is verplicht iedere derde aan wie de persoonsgegevens zijn verstrekt in kennis te stellen van elke rectificatie, tenzij dit onmogelijk is of onevenredig veel inspanning vraagt.

C. Recht op gegevenswissing (vergetelheid)

1. De Onderwijsinstelling is verplicht persoonsgegevens van de medewerker zonder onredelijke vertraging te wissen, onder andere indien:

* persoonsgegevens niet langer nodig zijn voor de doeleinden waarvoor zij zijn verzameld of anderszins verwerkt;
* de medewerker zijn toestemming intrekt en er geen andere rechtsgrond voor verwerking bestaat;
* de medewerker bezwaar maakt tegen de verwerking;
* de persoonsgegevens onrechtmatig verwerkt zijn.

D. Recht op beperking van de verwerking

1. De medewerker heeft het recht de Onderwijsinstelling te verzoeken zijn gegevens (tijdelijk) niet te verwerken / wijzigen indien:

* de medewerker de juistheid van persoonsgegevens betwist;
* de gegevens van de medewerker onrechtmatig worden verwerkt;
* de gegevens van de medewerker zijn niet meer nodig voor de verwerkingsdoeleinden;
* de medewerker bezwaar heeft gemaakt tegen de verwerking en in afwachting is van het antwoord op de vraag of de gerechtvaardigde gronden van verwerkingsverantwoordelijke zwaarder wegen dan die van de medewerker.

2. Het feit dat de verwerking van de persoonsgegevens beperkt is, moet door de Onderwijsinstelling duidelijk in het bestand zijn aangegeven zodat dit ook duidelijk is voor andere partijen.

3. Indien de verwerking is opgeschort, mogen de gegevens slechts met toestemming van de medewerker worden verwerkt.

4. Indien de Onderwijsinstelling de beperking wil opheffen dan dient de Onderwijsinstelling de medewerker hiervan op de hoogte te brengen.

E. Recht op overdraagbaarheid van gegevens

1. De medewerker heeft het recht om de gegevens die de medewerker aan de Onderwijsinstelling heeft verstrekt te ontvangen in een gestructureerde, gangbare en machineleesbare vorm.

2. De medewerker heeft daarnaast het recht om de verkregen gegevens aan een andere partij over te dragen zonder daarbij gehinderd te worden door de Onderwijsinstelling aan wie de persoonsgegevens eerder waren verstrekt.

F. Recht van bezwaar

1. De medewerker kan vanwege redenen die verband houden met zijn specifieke situatie bezwaar maken tegen de verwerking van zijn persoonsgegevens.

2. Als de medewerker bezwaar maakt dan staakt de Onderwijsinstelling de verwerking, tenzij dwingende gerechtvaardigde gronden anders bepalen.

## 3. Schending recht

1. Voor de uitoefening van de rechten doet de medewerker een schriftelijk verzoek aan de Functionaris voor de gegevensbescherming. De functionaris voor de gegevensbescherming zal dit verzoek doorzetten naar de daartoe aangewezen personen binnen de Onderwijsinstelling. Het College van Bestuur is de verantwoordelijke voor het besluit.

2. De Onderwijsinstelling bericht de medewerker zo spoedig mogelijk, doch uiterlijk binnen vier weken na ontvangst van het verzoek.

3. Indien een medewerker van mening is dat er sprake is van een ernstige schending van het Privacyreglement die hem direct raakt, dan wel de medewerker het niet eens is met de verwerking van zijn persoonsgegevens, dan kan hij zich wenden tot de Functionaris voor de gegevensbescherming.

## 4. Klachten

4.1. Indien de medewerker van mening is dat de bepalingen van de Verordening en overige wet-

en regelgeving en (onderwijs)gedragscodes zoals uitgewerkt in dit reglement niet door de instelling worden nageleefd dient hij/zij zich te wenden tot de FG.

4.2. Indien de ingediende klacht voor de betrokkene niet leidt tot een voor hem/haar acceptabel resultaat, kan hij zich wenden tot de Autoriteit Persoonsgegevens dan wel tot de rechter.

4.3. Medewerkers kunnen zich tevens wenden tot de externe klachtencommissie waarbij de [Stichting/Vereniging] is aangesloten [toevoegen: contactgegevens klachtencommissie].