PRIVACYREGLEMENT MEDEWERKERS

Voortgezet Onderwijs van Amsterdam

Uitgave	: ROC van Amsterdam
Auteur	: JZ
Kenmerk	: Privacyreglement Medewerkers VOvA
Vastgesteld door het College van Bestuur op	: 22-05-2018
Traject Platform OR ROCvA en OR ROCvF	: n.v.t.
Traject CSR ROCvA en ROCvF	: n.v.t.
Traject GMR VOvA	: 04-10-2018 ingestemd

Inhoudsopgave

Inleiding

Bij indiensttreding bij de Organisatie worden diverse persoonsgegevens vastgelegd. Persoonsgegevens liggen niet alleen vast in onze medewerkerssystemen maar door uitwisseling tussen diverse systemen worden automatisch ook gegevens overgedragen. De vraag hoe wij als Organisatie de privacy van onze medewerkers kunnen respecteren, en tegelijkertijd kunnen voldoen aan alle wettelijke verplichtingen die op ons als Organisatie rusten, is onverminderd een actueel thema.

Door de snelle technologische ontwikkelingen zijn nieuwe uitdagingen voor de bescherming van persoonsgegevens ontstaan en was de wetgeving toe aan vernieuwing. Op 25 mei 2018 is de Algemene Verordening Gegevensbescherming (hierna: AVG) in de gehele Europese Unie in werking getreden. Dit heeft tot gevolg dat de Nederlandse Wet bescherming persoonsgegevens niet meer geldt en ons Privacyreglement moest worden aangepast.

In dit Privacyreglement leggen wij vast wat de randvoorwaarden zijn voor onze Organisatie. Wij gaan zorgvuldig om met onze gegevens en met die van de medewerker. Daarnaast zullen wij niet onnodig inbreuk maken op iemands privacy en als wij gegevens uitwisselen met externe systemen en Organisaties dan doen wij dit aan de hand van in dit Privacyreglement vastgestelde richtlijnen.

Aldus vastgesteld op de op de voorzijde vermelde datum.

Voortgezet Onderwijs van Amsterdam

De heer E.C.M. de Jaeger
voorzitter College van Bestuur

Voortgezet Onderwijs van Amsterdam

Mevrouw L. Neuhaus
voorzitter Centrale directie

1. Algemene bepalingen

1. Uitleg belangrijkste begrippen

AVG:	Algemene Verordening Gegevensbescherming die op 25 mei 2018 in werking treedt voor geheel Europa en de Nederlandse Wet Bescherming Persoonsgegevens vervangt.
Bijzondere persoonsgegevens:	Een persoonsgegeven dat iets zegt over onder meer iemand zijn godsdienst, levensovertuiging, ras, politieke gezindheid en gezondheid, zoals bedoeld in artikel 9 AVG.
College van Bestuur:	Bevoegd gezag van de Organisatie o.g.v. art 1a sub 4 van de WVO en tevens verwerkingsverantwoordelijke.
Derde:	Iedereen die niet bij de verwerking van de persoonsgegevens betrokken is, zoals bijv. de Belastingdienst.
Logging gegevens:	Persoonsgegevens die onder meer onderstaande informatie bevatten: • locatie (waar je bent), • surfactiviteit (welke internetpagina's je bezoekt), • IP-adres (welk device je gebruikt, waar je bent) • inloggegevens (wie je bent).
Medewerker:	De persoon in dienst van de Organisatie over wie de persoons-gegevens iets zeggen.
Monitoring:	Monitoring is het bewaken van gegevens van de logging m.b.t. de ICT-voorzieningen.
Organisatie:	Het Voortgezet Onderwijs van Amsterdam.
Persoonsgegevens:	Alle geïdentificeerde of identificeerbare informatie over een natuurlijke persoon zoals bijvoorbeeld: • naam; • leeftijd; • geslacht, e-mail; • logging gegevens.
Privacy impact assessment (PIA):	Instrument om vooraf de privacy-risico'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.
Toestemming:	Ondubbelzinnige wilsuiting waarmee de medewerker 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 Organisatie persoonsgegevens verwerkt van medewerkers van de Organisatie.

Verwerkingsverantwoordelijke:	Het College van Bestuur van de Organisatie is eindverantwoordelijk voor de verwerking van persoonsgegevens binnen de Organisatie.
Verwerking van persoonsgegevens:	Alles wat met persoonsgegevens gedaan wordt, zoals verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, doorsturen etc..

2. Reikwijdte

1. Dit Privacyreglement gaat over het gebruik van persoonsgegevens van medewerkers.
2. Dit Privacyreglement biedt transparantie aan medewerkers over hoe de Organisatie 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.

3. Doel

Dit Privacyreglement heeft tot doel:
a. duidelijke richtlijnen voor omgang met persoonsgegevens;
b. toelichting 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.

4. Inwerkingtreding en duur

1. Het bevoegd gezag stelt het reglement vast na voorafgaande goedkeuring van de Gemeenschappelijke Medezeggenschapsraad (hierna: GMR).
2. Dit reglement treedt in werking op de op voorzijde van dit reglement vermelde datum voor de duur van 2 jaar.
3. Het Privacyreglement is gepubliceerd op de website van de Organisatie.

5. Wijziging

1. Het Privacyreglement kan tussentijds worden gewijzigd op verzoek van het College van Bestuur, de Functionaris Gegevensbescherming (hierna: FG) of de GMR.
2. Elke twee jaar vindt een evaluatie plaats en wordt onderzocht of het reglement naar tevredenheid van alle partijen werkt.
3. Indien partijen geen verzoek tot wijziging van het reglement aan de ander kenbaar hebben gemaakt, wordt het reglement van rechtswege verlengd voor de duur van twee jaar.
4. Indien een van de bepalingen uit dit reglement niet of niet meer geldig is, tast dit de geldigheid van het reglement niet aan. Het bestuur zal in dat geval zo snel mogelijk zorgdragen voor wijziging van het reglement.

6. Aanspreekbaarheid

1. De Organisatie 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 Organisatie zijn te allen tijde aanspreekbaar op het naleven van het privacyreglement.

7. Toepasselijk recht

1. Op dit reglement is het Nederlands recht van toepassing, de AVG wordt als Nederlands recht beschouwd.

8. Slotbepalingen

1. Dit Privacyreglement vervangt alle eerdere Privacyreglementen van de Organisatie.
2. In gevallen waarin dit reglement niet voorziet, beslist het College van Bestuur.

2. Verplichtingen van de Organisatie

1. Professioneel en integer handelen

1. De Organisatie spant zich in om op een zorgvuldige, veilige en vertrouwelijke manier met de persoonsgegevens om te gaan. Deze verplichting vervalt voor informatie die op basis van wettelijke verplichtingen moet worden aangeleverd.
2. De Organisatie spant zich in om:
   - de persoonlijke levenssfeer van de medewerker 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 Organisatie is verplicht om de onderstaande informatie aan de medewerker te verstrekken:
   - de identiteit van de Organisatie;
   - de doeleinden van de verwerking;
   - de contactgegevens van de vertegenwoordiger van de Organisatie;
   - 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 gegevensbescherming (FG)

1. De Organisatie heeft een FG aangesteld.
2. De FG vervult ten minste de onderstaande taken:
   - het registreren van verwerkingen van gegevensverwerkingen;
   - 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. Beveiligen, datalekken en Privacy Impact Assessment (PIA)

1. De Organisatie draagt zorg voor de nodige voorzieningen van fysieke, technische en organisatorische aard ter beveiliging van de persoonsregistraties.
2. De Organisatie zal een datalek zonder onredelijke vertraging, indien mogelijk uiterlijk 72 uur nadat zij hier kennis van heeft genomen, aan de Autoriteit Persoonsgegevens melden tenzij zij van mening is dat het datalek een risico inhoudt voor de rechten en vrijheden van de medewerkers.
3. De Organisatie informeert de medewerker over het datalek als het datalek ongunstige gevolgen heeft voor de persoonlijke levenssfeer van de medewerker.
4. Indien vereist zal de Organisatie een Privacy Impact Assessment (hierna: PIA) uitvoeren.

3. Persoonsgegevens

1. Persoonsgegevens

1. De Organisatie 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. Voor de categorie betrokkenen medewerkers in loondienst gelden de volgende categorieën van persoonsgegevens:
   1a. Contactgegevens beperkt
   1b. Contactgegevens volledig
   2. Personeelsnummer
   3. Nationaliteit
   4. Medische gegevens op eigen verzoek
   5. Godsdienst (n.v.t.)
   6. Financiën
   7. Beeldmateriaal
   8. Overige gegevens (o.a. ziekteverzuim)
   9. BSN
3. In het verwerkingsregister wordt vastgelegd welke gegevens van medewerkers worden vastgelegd en met welk doel.
4. Wijzigingen in wet- en regelgeving kunnen leiden tot het meer of minder vastleggen van gegevens.

2. Bijzondere persoonsgegevens

1. De Organisatie neemt de volgende persoonsgegevens niet op in haar systemen, tenzij dit op verzoek is van de medewerker:
   - godsdienst of levensovertuiging;
   - ras;
   - politieke gezindheid;
   - seksuele geaardheid en / of voorkeur;
   - strafrechtelijke persoonsgegevens.
2. Ten behoeve van de gezondheid of het welzijn van de medewerker worden de gegevens die de Organisatie noodzakelijk acht om haar doelstelling te bereiken vastgelegd in het personeelsdossier.
3. Het personeelsdossier van een medewerker wordt bewaard op een afgesloten plaats / afgeschermde digitale plek.

3. Wijze van verkrijgen van persoonsgegevens

1. De persoonsgegevens worden voor zover mogelijk door de medewerker zelf verstrekt bij de sollicitatie en /of ondertekening van de arbeidsovereenkomst.
2. De persoonsgegevens worden door de daartoe bevoegde en geautoriseerde medewerkers in het personeelssysteem gezet en onderhouden.
3. De medewerker is verantwoordelijk voor het tijdig aanleveren en voor de juistheid van de gegevens.
4. Indien de Organisatie extra informatie nodig heeft over de medewerker zal zij deze uitsluitend met schriftelijke toestemming van de medewerker opvragen, tenzij deze niet vereist is.

4. Aanmelden op ICT-voorzieningen van de Organisatie

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 niet anoniem gebruik gemaakt kan worden van de ICT-voorzieningen en de internetverbinding van de Organisatie. Dat betekent dat men zich altijd moet aanmelden voordat gebruik kan worden gemaakt van een ICT-voorziening (computer, telefoon, WIFI, Portaal voor Talent etc.).
3. In de Gedragscode ICT heeft de Organisatie vastgelegd wat de randvoorwaarden zijn voor het gebruik van onze ICT-voorzieningen.
4. Elke medewerker wordt geacht de inhoud van de Gedragscode ICT te kennen en zich hieraan te houden.

5. Monitoring

1. Aanmelden op een ICT-voorziening houdt automatisch in dat 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 Organisatie 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 de Gedragscode ICT raadplegen.

4. Verwerken van persoonsgegevens

1. Verwerken van persoonsgegevens

1. Bij de verwerking van persoonsgegevens houdt de Organisatie zich aan de wet.
2. De verwerking van persoonsgegevens vindt plaats onder meer door:

A. Uitvoering van de arbeidsovereenkomst
- het betalen van het salaris;
- het komen tot een aanstelling.

B. Wettelijke plicht:
- het laten uitvoeren van accountantscontrole;
- gegevens verstrekken aan organisaties zoals de belastingdienst, pensioenfonds e.d.;
- de begeleiding in het kader van de Wet Gelijke behandeling gehandicapte en chronisch zieke medewerkers.
- de uitvoering of toepassing van een andere wet.

C. Gerechtvaardigd belang:
- cameratoezicht.

2. Toegang tot de persoonsregistratie en beveiliging

1. De Organisatie zorgt ervoor dat de toegang tot de administratie en systemen beperkt is. Slechts personen binnen de Organisatie, die als gevolg van hun taak daartoe gerechtigd zijn, hebben rechtstreeks toegang tot de persoonsregistraties, met dien verstande dat deze bevoegdheid zich slechts uitstrekt tot het gebruik van de opgenomen gegevens voor doeleinden die met het doel van de betreffende persoonsregistratie verenigbaar zijn.
2. Iedereen die binnen de Organisatie persoonsgegevens verwerkt, is verplicht daar vertrouwelijk mee om te gaan.
3. De Organisatie 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, tenzij hiervoor een wettelijk verplicht gestelde bewaartermijn geldt.
2. De Organisatie spant zich in zich te houden aan de wettelijke vernietiging en bewaartermijnen.
3. Indien de bewaartermijn is verstreken, worden desbetreffende persoonsgegevens binnen een redelijke termijn uit de registratie verwijderd of vernietigd.
4. Vernietiging blijft evenwel achterwege wanneer:
   - redelijkerwijs aannemelijk is dat de bewaring van aanmerkelijk belang is voor een ander dan de medewerker;
   - de zorg van een goede administratie of rechtszaak bewaring noodzaakt;
   - bewaring op grond van een wettelijk voorschrift vereist is;
   - indien daarover tussen de medewerker en de organisatie 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.

5. Richtlijnen verstrekking van persoonsgegevens

1. Grondslag

De voornaamste redenen voor het verstrekken van gegevens aan derden zijn:

A. Uitvoering wettelijke plicht
De Organisatie is gebonden aan onderwijswetgeving, deze maakt het noodzakelijk om in bepaalde situaties persoonsgegevens van medewerkers aan externe partijen te verstrekken.
- voor het doen verrichten van accountants- en inspectiecontroles;
- politieonderzoek.

B. Gerechtvaardigd belang

1. De Organisatie zal persoonsgegevens mogen verwerken en uitwisselen voor zover dit 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 van de medewerker voor gaat. De Organisatie moet hier een belangenafweging maken.

2. Op grond van het gerechtvaardigd belang kunnen onder meer persoonsgegevens aan derden verstrekt worden voor zover dit noodzakelijk is:
   - met het oog op begeleiding van de medewerker;
   - voor het in handen van derden stellen van vorderingen;
   - voor het behandelen van geschillen.

C. Toestemming van de medewerker

3. Mocht geen gerechtvaardigd belang aanwezig zijn, dan wel uit de onder B bedoelde belangenafweging is gebleken dat het belang van de medewerker dient te prevaleren, zal de verstrekking van persoonsgegevens alleen mogen plaatsvinden met toestemming van de medewerker.

2. Juridische toetsing van verzoeken

1. Elke verstrekking van persoonsgegevens moet, naast het hebben van een grondslag, voldoen aan de volgende eisen:

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

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

C. Dataminimalisatie
De Organisatie verstrekt niet langer en ook niet meer gegevens dan noodzakelijk is voor het dienen van het belang van de derde. De Organisatie verstrekt dan ook niet de volledige administratie maar alleen dat gedeelte waarmee de derde haar doel kan bereiken.

3. Schriftelijke afspraken over gegevensverstrekking

1. Wanneer de Organisatie persoonsgegevens, al dan niet op regelmatige basis, aan een derde verstrekt, maken partijen hierover schriftelijke afspraken.
2. Wanneer de Organisatie een derde inschakelt die de persoonsgegevens namens haar verwerkt, zal zij daarmee een (verwerkers)overeenkomst afsluiten.

6. Rechten van de medewerkers

1. Rechten van de medewerker

1. Op basis van de wet en dit Privacyreglement heeft de medewerker een aantal rechten.
2. Een medewerker heeft in ieder geval recht op inzage in zijn / haar (hierna: zijn) personeelsdossier en, indien van toepassing, recht op correctie van onjuiste gegevens die aldaar zijn opgenomen.
3. Voor de uitoefening van de rechten genoemd in dit hoofdstuk, doet de medewerker een schriftelijk en / of mondeling verzoek aan afdeling Personeelszaken.
4. De Organisatie bericht de medewerker zo spoedig mogelijk, doch uiterlijk binnen vier weken, na ontvangst van het verzoek.

2. Inzage persoonsgegevens

A Recht van inzage

1. De medewerker heeft het recht te weten of, en zo ja welke, persoonsgegevens worden verwerkt door de organisatie.
2. De Organisatie draagt ervoor zorg dat een medewerker online inzage heeft in zijn personeelsdossier.
3. Indien een medewerker inzage wenst van persoonsgegevens die niet (meer) online inzichtelijk zijn, dient hij schriftelijk een verzoek in te dienen bij de directie van het organisatieonderdeel waar hij werkzaam is.
4. De Organisatie verstrekt de medewerker zo spoedig mogelijk, doch uiterlijk binnen vier weken, na ontvangst van het verzoek tot inzage een kopie van de persoonsgegevens die worden verwerkt. Aan een verzoek om bijkomende kopieën kunnen kosten worden verbonden.
5. Voordat een medewerker inzage krijgt in zijn dossier dient de medewerker zich te legitimeren.
6. De Organisatie draagt steeds zorg voor een deugdelijke vaststelling van de identiteit van de medewerker.

3. Correctie persoonsgegevens

B. Recht op rectificatie

7. De medewerker heeft recht op verbetering, aanvulling of verwijdering van op hem betrekking hebbende persoonsgegevens indien deze niet correct zijn.
8. De Organisatie 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)

9. De Organisatie zal persoonsgegevens van de medewerker zonder onredelijke vertraging 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 geen andere rechtsgrond voor verwerking bestaat;
   - de medewerker bezwaar maakt tegen de verwerking;
   - de persoonsgegevens onrechtmatig verwerkt zijn.
10. De sollicitant / persoon die niet is aangenomen door de Organisatie kan een verzoek doen bij de Organisatie om zijn gegevens te laten verwijderen. De Organisatie verwijdert binnen de wettelijk gestelde termijn van 4 weken de gegevens van de niet aangenomen sollicitant / persoon.

D. Recht op beperking van de verwerking

1. De medewerker heeft het recht de Organisatie 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 niet meer nodig zijn voor de verwerkingsdoeleinden;
   - de betrokkene 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 het recht op de verwerking van de persoonsgegevens is beperkt moet duidelijk door de Organisatie 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 Organisatie de beperking wil opheffen dient de organisatie 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 Organisatie heeft verstrekt te ontvangen in een gestructureerde, gangbare en machine leesbare 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 Organisatie 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 organisatie de verwerking, tenzij dwingende gerechtvaardigde gronden anders bepalen.

4. Rechtsbescherming

A. Intern

1. Indien een sollicitant van mening is dat zijn privacy is geschonden door de Organisatie, dan kan hij een klacht indienen bij het College van Bestuur / de FG van de Organisatie.
2. Indien een medewerker van mening is dat zijn privacy is geschonden door de Organisatie, dan wel de medewerker het niet eens is met de registratie van zijn persoonsgegevens, dan heeft hij onderstaande mogelijkheden:
   - melding doen bij de FG;
   - inschakelen van een Vertrouwenspersoon / de Ombudsman;
   - een schriftelijke klacht indienen bij de directie van het organisatieonderdeel waar hij werkzaam is;
   - een schriftelijke klacht indienen bij de Klachtencommissie Medewerkers;
3. In de reglementen van respectievelijk de FG, de Vertrouwenspersoon, de Ombudsman en de Klachtencommissie Medewerkers staat beschreven hoe men een klacht kan indienen en wat de procedure is.

B. Extern

4. Het staat een medewerker vrij om een klacht in te dienen bij de Autoriteit Persoonsgegevens dan wel de rechter indien interne conflictoplossing niet tot een voor hem bevredigende oplossing heeft geleid.