Privacy Expertise Centrum

← hier het logo van jouw organisatie

# Privacyreglement medewerkers

Kaders voor de verwerking van persoonsgegevens

# Colofon

Dit document bevat het privacyreglement voor medewerkers van [Organisatie]. Dit document vloeit voort uit het Strategisch Privacybeleid en beschrijft de kaders/richtlijnen voor de verwerking van persoonsgegevens (een 'standaard' uit de beleidspiramide). Het kan worden gebruikt bij het SURF Toetsingskader Privacy, domein 'Beleid' (BL.01). Deze richtlijnen vormen ook de kaders voor de invulling van privacyverklaringen voor specifieke verwerkingen (zoals de privacyverklaring op de website van onze organisatie).

## Bestemd voor

Dit document is bestemd voor medewerkers van [Organisatie].

## Samenstelling en beheer

Dit document is gebaseerd op een template dat tot stand is gekomen via het Privacy Expertise Centrum van SURF. Het beheer van het template berust bij SURF.

## Licentie



**Versiebeheer**

| Versie | Door | Datum | Toelichting/wijziging |
|---|---|---|---|
| 1.0 | SURF | 11-08-2026 | Initieel document |
| | | | |
| | | | |
| | | | |
| | | | |

# Inhoudsopgave

# Inleiding

[Organisatie] (hierna '[Organisatie]) wil medewerkers een veilige werkplek bieden. Een randvoorwaarde daarvoor is het goed en zorgvuldig omgaan met persoonsgegevens binnen de school. In dit privacyreglement legt [Organisatie] die randvoorwaarden vast.

De Algemene Verordening Gegevensbescherming (AVG) stelt allerlei eisen aan hoe we met persoonsgegevens moeten omgaan.

Dit reglement verwoordt de manier waarop [Organisatie] de verwerking van persoonsgegevens volgens de AVG, de Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG), sectorgedragscodes, sectorbeveiligingscodes en organisatie-specifieke (interne) regelingen laat plaatsvinden.

Dit gaat bijvoorbeeld over:

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

[Organisatie] maakt geen onrechtmatige inbreuk op iemands privacy. Als [Organisatie] persoonsgegevens van medewerkers uitwisselt met externen dan doet [Organisatie] dat binnen de geldende wet- en regelgeving en aan de hand van de in dit privacyreglement nader uitgewerkte richtlijnen.

Het bestuur legt in samenspraak met de Privacy Officer en Functionaris voor Gegevensbescherming (FG) passende maatregelen ten uitvoer en legt verantwoording af over het gevoerde beleid aan de medezeggenschapsorganen en de Raad van Toezicht van [Organisatie].

# Hoofdstuk 1 Algemene bepalingen

## Artikel 1 Uitleg belangrijkste begrippen (alfabetisch)

Specifieke begrippen die hieronder worden toegelicht, hebben betrekking op de definities zoals bedoeld in de AVG.

| | |
|---|---|
| Autoriteit Persoonsgegevens | De toezichthoudende autoriteit van Nederland, zoals bedoeld in de AVG, ook wel 'AP' genoemd. |
| AVG | Algemene verordening gegevensbescherming van 27 april 2016. |

| | |
|---|---|
| Bijzondere persoonsgegevens | Persoonsgegevens van een bijzondere categorie, zoals gegevens over gezondheid en persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen blijken, zoals bedoeld in de AVG. |
| Datalek | een inbreuk op de beveiliging bij [Organisatie]die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens. |
| [Organisatie] | [volledige naam organisatie], gevestigd te [Plaats], dan wel haar bestuur of gevolmachtigde(n), de zogenaamde 'verwerkingsverantwoordelijke', zoals bedoeld in de AVG. |
| Derde | Iedereen die niet bij de verwerking van persoonsgegevens is betrokken, zoals een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan (niet zijnde de medewerker, [Organisatie], verwerker of de personen die onder rechtstreeks gezag van [Organisatie] of de verwerker gemachtigd zijn om de persoonsgegevens te verwerken), zoals leerplichtambtenaren, DUO etc., zoals bedoeld in de AVG |
| Privacybeoordeling | instrument om vooraf de privacyrisico's van een verwerking in kaart te brengen zodat helder wordt welke maatregelen moeten worden genomen om de risico's te verkleinen, waaronder de Data Protection Impact Assessment (DPIA) c.q. de zogenaamde 'gegevensbeschermingseffectbeoordeling' zoals bedoeld in de AVG |
| Functionaris voor gegevensbescherming | De interne toezichthouder (zoals bedoeld in de AVG) bij [Organisatie], ook wel 'FG' genoemd |
| Gegevensbescherming | De technische en organisatorische maatregelen die worden genomen om te voorzien in het fundamentele recht op bescherming van persoonsgegevens als deze door anderen moeten worden gebruikt. |
| Medewerker | Degene die voor en/of namens [Organisatie] werkzaamheden verricht (via een arbeids- en/of uitzendovereenkomst, detachering als stagiair of op een andere manier) |

| | |
|---|---|
| Monitoring en logging | Het bewaken van en het vastleggen van gebeurtenissen in de netwerkinfrastructuur van [Organisatie] |
| Persoonsgegevens | Alle informatie die te herleiden is naar een natuurlijke persoon, zoals naam, leeftijd, geslacht etc. Hieronder vallen ook digitale persoonsgegevens, zoals het IMEI-nummer van de smartphone, locatiegegevens, etc. |
| Privacy | Privacy wordt 'eerbiediging van de persoonlijke levenssfeer' genoemd in artikel 10 lid 1 Grondwet |
| Privacy Officer | De medewerker die zich bezighoudt met het vertalen en uitvoeren van wet- en regelgeving op het gebied van privacy op proces- en systeemniveau, ook wel 'PO' genoemd. |
| Toestemming | Elke vrije, specifieke, geïnformeerde wilsuiting waarmee medewerkers door middel van een verklaring of een actieve handeling de verwerking van hun persoonsgegevens accepteert. |
| UAVG | Uitvoeringswet Algemene verordening gegevensbescherming van 16 mei 2018. |
| Verwerker | Degene die voor [Organisatie] persoonsgegevens verwerkt. |
| Verwerking van persoonsgegevens | Alles wat met persoonsgegevens wordt gedaan, zoals het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, doorsturen, etc., al dan niet geautomatiseerd uitgevoerd. |
| Verwerkingsregister | Register met verwerkingsactiviteiten, zoals bedoeld in de AVG, ook wel 'dataregister' genoemd. |

## Artikel 2 Totstandkoming privacyreglement

1. Dit privacyreglement is na instemming van de [naam medezeggenschapsorgaan] vastgesteld door [Organisatie].

2. Dit privacyreglement vervangt alle eerdere versies van dit privacyreglement van [Organisatie].

3. In situaties waarin dit privacyreglement geen uitsluitsel verschaft, beslist [Organisatie].

### Artikel 3 Inwerkingtreding privacyreglement

Het privacyreglement treedt in werking met ingang van [datum]

### Artikel 4 Reikwijdte privacyreglement

1. Dit privacyreglement gaat over het gebruik van persoonsgegevens van medewerkers en sollicitanten bij [Organisatie].

2. In dit privacyreglement wil [Organisatie]met een aantal regels openheid bieden over hoe [Organisatie]omgaat met persoonsgegevens van medewerkers.

3. Dit privacyreglement is niet van toepassing op persoonsgegevens opgenomen in bestanden van de vertrouwenspersoon, de Ondernemingsraad en de Interne Klachtencommissie. De vertrouwelijkheid van deze gegevens is geregeld in desbetreffende regelingen en in de AVG.

4. Als er bepalingen uit dit reglement strijdig zijn met geldende wet- en regelgeving, dan gaan de betreffende bepalingen uit die wet- en regelgeving vóór de bepalingen uit dit reglement.

5. Als persoonsgegevens zo zijn bewerkt dat ze niet tot natuurlijke personen ter herleiden zijn, is er sprake van geanonimiseerde gegevens. Deze gegevens vallen niet onder de reikwijdte van de AVG en ze kunnen daarom in deze geanonimiseerde vorm bewaard blijven.

### Artikel 5 Doel privacyreglement

Met dit privacyreglement wenst [Organisatie]:

a. de privacy van de medewerker te beschermen tegen verkeerd, onzorgvuldig 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;
d. de privacyrechten van de medewerker te waarborgen.

### Artikel 6 Aanspreekbaarheid

1. [Organisatie] en haar medewerkers worden geacht de inhoud van dit privacyreglement te kennen en zich hieraan te houden.

2. Medewerkers kunnen [Organisatie] altijd aanspreken op het (niet) naleven van dit privacyreglement.

3. Dit privacyreglement is gepubliceerd op het intranet van [Organisatie].

## Hoofdstuk 2 Verplichtingen van [Organisatie]

### Artikel 7 Professioneel en integer handelen

1. [Organisatie] gaat op een zorgvuldige, veilige en vertrouwelijke manier met de persoonsgegevens om volgens de geldende wetgeving.

2. [Organisatie] spant zich in om doelen zoals genoemd in artikel 5 ‘Doel privacyreglement’ van dit reglement te behalen.

## Artikel 8 Informeren van medewerkers

[Organisatie] is verplicht om medewerkers helder te informeren over de persoonsgegevens die over hen wordt verzameld en over wat hun rechten zijn rondom verwerking daarvan. Het gaat onder andere over:

- het doel van de verwerking(en);
- met wie de persoonsgegevens worden gedeeld;
- de bewaartermijn van de persoonsgegevens;
- het recht op inzage, vergetelheid;
- het recht om een klacht in te dienen (zie artikel 30 ‘Uitoefening rechten door medewerker’ van dit reglement);
- andere informatie waar dat nodig is om een zorgvuldige verwerking te garanderen;
- de contactgegevens van de Privacy Officer en Functionaris voor Gegevensbescherming.

## Artikel 9 Functionaris voor Gegevensbescherming en Privacy Officer

1. [Organisatie] heeft een Functionaris voor Gegevensbescherming (FG) en een Privacy Officer aangewezen.

2. De FG vervult onder andere de onderstaande taken op het gebied van privacy:

    - toezicht houden op de naleving van wet- en regelgeving en de naleving van het privacyreglement;
    - algemene adviesrol met betrekking tot gegevensverwerking, waaronder de afhandeling van klachten, zoals bedoeld in artikel 27, lid 3 ‘Uitoefening rechten door medewerker’ van dit reglement;
    - het bewustmaken en trainen van medewerkers;
    - vaste deelnemer van het datalekteam dat actief wordt wanneer er een datalek is geconstateerd en eerste contactpersoon van de AP (zie artikel 12 ‘Datalekken’ van dit reglement).

3. De Privacy Oficer vervult onder andere de onderstaande taken op het gebied van privacy:

    - adviseren over privacybestendige uitvoering van gegevensverwerkingen;
    - het mede ontwikkelen/actueel houden van reglementen en beleid;
    - het ontwikkelen en actueel houden van procedures;
    - het bewustmaken en trainen van medewerkers;
    - het voeren van incidentmanagement op privacygebied;
    - het opstellen van het jaarplan privacy;
    - het rapporteren over de uitvoering van het privacybeleid en het jaarplan;
    - het ondersteunen bij privacybeoordelingen zoals DPIA’s en het definiëren en helpen implementeren van maatregelen;
    - compliancechecks van software/faciliterende ICT-systemen.
    - centraal punt voor vragen over de AVG en het privacybeleid van [Organisatie].

### Artikel 10 Beveiligen

[Organisatie] zorgt voor de benodigde, moderne voorzieningen van fysieke, technische en organisatorische aard om verlies of onrechtmatige verwerking van persoonsgegevens te voorkomen. Het strategisch beleid voor informatiebeveiliging en privacy en het ICT-reglement van [Organisatie] verwoorden de invulling daarvan, zoals de ICT-beveiliging, risicoanalyses en de afhandeling van incidenten.

### Artikel 11 Data Protection Impact Assessment

De AVG omschrijft de situaties waarin het verplicht is een DPIA als privacybeoordeling uit te voeren en de AP geeft daar nader invulling gaan. [Organisatie] bepaalt op basis van hiervan of een DPIA moet worden uitgevoerd (via een pre-scan DPIA). Op basis van de uitkomst van andere manieren van risico-inschatting (zoals een privacyclassificatie of een BIV-classificatie (Beschikbaarheid, Integriteit, Vertrouwelijkheid) kan de organisatie bepalen ervoor te kiezen een DPIA uit te voeren, ook als dit niet wettelijk verplicht is.

### Artikel 12 Datalekken

Voor de afhandeling van (mogelijke) datalekken bij [Organisatie] werkt de organisatie volgens de standaard ‘Richtlijnen omgaan met datalekken’ en de Datalekprocedure. Deze richtlijnen en het datalekprotocol voorzien in de adequate afhandeling van datalekken, afgestemd op de situatie. De Kerngroep Datalekken die daarin is vermeld, volgt de richtlijnen en de werkwijze zoals beschreven in het datalekprotocol.

## Hoofdstuk 3 Persoonsgegevens

### Artikel 13 Persoonsgegevens

1. [Organisatie] streeft bij het verwerken van persoonsgegevens naar dataminimalisatie: er worden niet meer persoonsgegevens vastgelegd dan nodig. Dit houdt in dat alleen persoonsgegevens worden verwerkt die redelijkerwijs nodig zijn om het betreffende doel te bereiken.

2. [Organisatie] verwerkt persoonsgegevens van de medewerker zoals opgenomen in haar verwerkingsregister. In hoofdlijnen gaat het om persoonsgegevens die nodig zijn voor uitvoering van de arbeidsovereenkomst. Zie ook hoofdstuk 4 van dit reglement.

3. Wijzigingen in wet- en regelgeving kunnen leiden tot het vastleggen van meer of minder persoonsgegevens. Nieuwe verwerkingsprocessen of wijzigingen in bestaande verwerkingsprocessen vinden uitsluitend plaats als er een wettelijke grondslag voor de verwerking is. Deze worden zo snel mogelijk in het verwerkingsregister geregistreerd.

4. Ook voor andere situaties kan er sprake zijn van gegevensverwerking, zoals bij de organisatie van evenementen, registratie van oud-medewerkers, etc. [Organisatie] verwerkt ook in die situaties uitsluitend persoonsgegevens op basis van een van de wettelijke grondslagen.

5. [Organisatie] zorgt voor publicatie van het verwerkingsregister.

### Artikel 14 Bijzondere persoonsgegevens

1. [Organisatie] neemt geen bijzondere (zoals gezondheidsgegevens en biometrische gegevens), etc.) of strafrechtelijke persoonsgegevens of op in haar systemen, tenzij dit noodzakelijk is voor [Organisatie] – in het belang van de medewerker – en mits daarvoor in wet- en regelgeving een uitzondering wordt gegeven en er sprake is van een wettelijke grondslag.

### Artikel 15 Wijze van verkrijgen van persoonsgegevens

1. De persoonsgegevens van de medewerker worden voor zover mogelijk door de medewerker zelf verstrekt.

2. De persoonsgegevens worden door de daartoe bevoegde en geautoriseerde medewerkers in de daarvoor bestemde systemen gezet en onderhouden.

3. De medewerker is zelf verantwoordelijk voor het tijdig aanleveren van de gegevens en voor de juistheid daarvan.

### Artikel 16 Aanmelden op ICT-voorzieningen van [Organisatie]

1. Het Informatiebeveiligingsbeleid van [Organisatie] bepaalt dat er geen anoniem gebruik van de ICT-voorzieningen en de internetverbinding van [Organisatie] kan worden gemaakt. Dat betekent dat men zich altijd moet aanmelden met een persoonlijk inlogaccount voordat men de ICT-voorzieningen kan gebruiken (zoals computer, telefoon, wifi, etc.).

2. Het ICT-reglement Medewerkers bepaalt onder welke voorwaarden de medewerker de ICT-voorzieningen kan gebruiken.

3. Elk medewerker wordt geacht de inhoud van dit ICT-reglement te kennen en zich hieraan te houden.

4. Het ICT-reglement is door de medewerker in te zien op het intranet van [Organisatie].

### Artikel 17 Monitoring en logging

Voor de ICT-voorzieningen maakt [Organisatie] gebruik van tools voor monitoring van het netwerk en logging van het ICT- en internetgebruik. Deze tools worden alleen gebruikt voor handhaving van het ICT-reglement, de goede werking en beveiliging van de ICT-voorzieningen en/of het voorkomen of oplossen van ongeregeldheden binnen het netwerk (zie het ICT-reglement).

## Hoofdstuk 4 Verwerken van persoonsgegevens

### Artikel 18 Verwerken van persoonsgegevens

1. Bij de verwerking van persoonsgegevens houdt [Organisatie] zich aan de geldende wet- en regelgeving.

2. De verwerking van persoonsgegevens vindt plaats op basis van onder meer de volgende wettelijke grondslagen:

   a. Uitvoering van de overeenkomst
   Voor het uitvoeren van de arbeidsovereenkomst moet [Organisatie] verschillende persoonsgegevens verwerken, bijvoorbeeld voor:
   - de personeelsadministratie,
   - het uitbetalen van het salaris;
   - het vastleggen van afspraken en gegevens rondom functioneren en beoordeling;
   - de administratie van declaraties en vergoedingen;
   - uitkering bij ontslag.

   b. Wettelijke plicht
   [Organisatie] moet zich houden aan diverse wet- en regelgeving, zoals:
   - onderwijswetgeving;
   - titel 7.10 van het Burgerlijk Wetboek;
   - Arbeidsomstandighedenwet (gegevensuitwisseling arbodienst);
   - Archiefwet);
   - belastingwetgeving (bijvoorbeeld de accountantscontrole).

   c. Gerechtvaardigd belang
   In sommige situaties heeft [Organisatie] gerechtvaardigde belangen voor de verwerking van persoonsgegevens, bijvoorbeeld bij:
   - screening en communicatie sollicitanten;
   - contact met oud-personeelsleden;
   - videocameratoezicht (volgens het reglement Videocameratoezicht).

   d. Toestemming
   Als er geen sprake is van een andere wettelijke grondslag, kan toestemming als grondslag worden gebruikt, bijvoorbeeld voor vermelding op een verjaardagslijst of adreslijst voor lief en leed op de afdeling.

3. [Organisatie] zet geen geautomatiseerde individuele besluitvorming of profilering in bij de verwerking van persoonsgegevens van medewerkers.

4. De grondslagen voor uitwisseling van gegevens aan derden zijn nader uitgewerkt in artikel 21 ‘Grondslag uitwisseling’ van dit reglement.

## Artikel 19 Toegang tot de persoonsregistratie en beveiliging

1. [Organisatie] zorgt ervoor dat de toegang tot de administratie en de systemen beperkt is. Medewerkers hebben slechts toegang tot persoonsgegevens als dat voor de uitvoering van hun functie nodig is. De rechten en rollen voor deze toegang zijn vastgelegd in een autorisatieschema.

2. Iedereen die voor of namens [Organisatie] persoonsgegevens verwerkt, is verplicht daar vertrouwelijk mee om te gaan.

3. Iedereen die betrokken is bij de uitvoering van dit reglement en daarbij de beschikking krijgt over persoonsgegevens waarvan men het vertrouwelijke karakter kent of redelijkerwijs kan vermoeden en voor wie niet uit hoofde van beroep, functie of wettelijk voorschrift ter zake van de persoonsgegevens een geheimhoudingsplicht geldt, is verplicht tot geheimhouding daarvan. Dit geldt niet als enig wettelijk voorschrift die bekendmaking verplicht maakt of als dit uit de taak bij de uitvoering van dit reglement de noodzaak tot bekendmaking voortvloeit.

4. Derden die voor of namens [Organisatie] persoonsgegevens verwerken, zijn verplicht tot geheimhouding daarvan en moeten in het kader daarvan een geheimhoudingsverklaring ondertekenen.

5. De verwerker en derden hebben toegang tot persoonsgegevens als:

   - degene die betrokken is bij of belast is met het leidinggeven aan de verwerkingsactiviteiten;
   - de verwerker die door [Organisatie] gemachtigd is om persoonsgegevens te verwerken;
   - er op grond van een wet toegang moet worden verleend;
   - [Organisatie] daarvoor een gerechtvaardigd belang heeft.

6. In bijzondere situaties, zoals bij overlijden, langdurige ziekte, arbeidsongeschiktheid of afwezigheid of andere zwaarwegende reden(en), kan [Organisatie] toegang tot de bestanden of mailbox van de betreffende medewerker toestaan volgens de voorwaarden in het ICT-reglement.

## Artikel 20 Bewaren en verwijderen van persoonsgegevens

1. Persoonsgegevens worden niet langer bewaard dan nodig. Daarbij wordt rekening gehouden met wettelijke bewaar- en vernietigingstermijnen, waaronder selectielijsten. Deze bewaartermijnen worden binnen [Organisatie] vastgelegd.

2. Als de bewaartermijn is verstreken worden de desbetreffende persoonsgegevens binnen een redelijke termijn verwijderd c.q. vernietigd. Onder verwijderen en vernietigen wordt ook anonimiseren verstaan, zoals verwoord in artikel 4, lid 5 van dit reglement.

3. Persoonsgegevens worden niet vernietigd als:

   - er een noodzaak is om ze te bewaren in verband met de zorg van een goede administratie of de afhandeling van een geschil of rechtszaak;
   - er een gerechtvaardigd belang is om gegevens langer te bewaren voor onderzoeksdoeleinden volgens de afspraken die daarover binnen [Organisatie] zijn gemaakt.

# Hoofdstuk 5 Verstrekking van persoonsgegevens

## Artikel 21 Grondslag uitwisseling

1. Het verstrekken van gegevens aan derden gebeurt alleen als dat nodig is op basis van een wettelijke grondslag (zie hoofdstuk 6, Derden waaraan persoonsgegevens worden verstrekt). De meestvoorkomende grondslagen zijn:

   Uitvoering wettelijke plicht
   [Organisatie] is gebonden aan de geldende wet- en regelgeving, zoals de onderwijswetgeving. Deze wetgeving verplicht de organisatie om in bepaalde situaties persoonsgegevens van medewerkers aan externe partijen door te geven.

   Uitvoering overeenkomst
   [Organisatie] is verantwoordelijk voor een goede uitvoering van de arbeidsovereenkomst. Dit betekent dat [Organisatie] persoonsgegevens aan externe partijen mag doorgeven als dit noodzakelijk is voor de uitvoering van die overeenkomst.

   Gerechtvaardigd belang
   [Organisatie] mag persoonsgegevens doorgeven aan derden als dat noodzakelijk is voor het gerechtvaardigd belang van de organisatie (bijvoorbeeld het verstrekken zakelijke telefoonnummers of e-mailadressen van een medewerker voor contact met externen) of van een derde (bijvoorbeeld aan de politie op haar verzoek als er nog geen sprake is van een wettelijke verplichting). Het gaat hier om handelingen die vallen onder de normale bedrijfsvoering of het dagelijks beheer van de organisatie. [Organisatie] moet zich wel afvragen of met anonieme en/of met minder gegevens of via een minder ingrijpende weg hetzelfde resultaat kan worden bereikt. Ook moet [Organisatie] een privacybeoordeling uitvoeren. Dit betekent dat [Organisatie] het belang van de medewerker moet afwegen tegen het belang van de organisatie zelf bij het verstrekken van de gegevens.

   Vitaal belang
   [Organisatie] mag persoonsgegevens doorgeven aan derden als dat voor de medewerker een levensreddende handeling kan zijn, bijvoorbeeld als de medewerker buiten bewustzijn is.

   Toestemming van de medewerker
   Als geen van bovenstaande criteria van toepassing is, mag de verstrekking van persoonsgegevens alleen plaatsvinden met de (aantoonbare) toestemming van de medewerker. Die toestemming moet aan de wettelijk eisen van de AVG voldoen en kan niet worden gevraagd als er sprake is van een machtsverhouding.

2. Als de persoonsgegevens (aantoonbaar) zijn geanonimiseerd en dus niet terug te leiden zijn tot een individu, kan de verantwoordelijke beslissen deze zowel binnen als buiten [Organisatie] te verstrekken voor wetenschappelijk onderzoek en statistiek.

## Artikel 22 Juridische toetsing van verzoeken om informatie

Voor elke verwerking en verstrekking van persoonsgegevens op basis van een van de noodzakelijkheidsgrondslagen (alle wettelijke grondslagen zoals bedoeld in artikel 21 behalve de grondslag 'toestemming'), geldt dat deze ook de noodzakelijkheidstoets moeten doorstaan. Daarvoor gelden de volgende eisen:

a. Subsidiariteit
   Het doel waarvoor de persoonsgegevens worden verwerkt kan in redelijkheid niet op een andere manier worden gerealiseerd.

b. Proportionaliteit en doeltreffendheid
   Met de verwerking wordt het gestelde doel behaald en dit staat in verhouding tot het feit dat hiervoor persoonsgegevens moeten worden verwerkt (de inbreuk op de belangen van de medewerker mag niet onevenredig groot zijn in verhouding tot het doel).

c. Dataminimalisatie
   [Organisatie] verzameld en verstrekt niet meer gegevens dan nodig. Zo verstrekt [Organisatie] bijvoorbeeld niet de volledige administratie van een bepaalde verwerking, maar alleen dat gedeelte ervan waarmee het beoogde doel kan worden bereikt.

d. Veiligheid
   Als bijzondere persoonsgegevens deel uitmaken van de gegevensverstrekking, moet [Organisatie] extra (passende, proportionele) waarborgen voor veilige uitwisseling treffen. Denk aan moderne encryptietechnieken en uitwisseling via een veilig platform voor bestandsuitwisseling.

## Artikel 23 Schriftelijke afspraken over gegevensverstrekking

1. Wanneer [Organisatie] persoonsgegevens, al dan niet op regelmatige basis, aan een derde verstrekt, maken partijen hierover schriftelijke afspraken, bijvoorbeeld via een gegevensuitwisselingsovereenkomst.

2. Wanneer [Organisatie] een verwerker inschakelt om persoonsgegevens namens [Organisatie] te verwerken, sluit de organisatie een verwerkersovereenkomst met de verwerker af.

3. Op de schriftelijke afspraken zoals vermeld lid een en twee van dit artikel, zijn de artikelen 21 en 22 van dit reglement van toepassing.

# Hoofdstuk 6 Derden waaraan persoonsgegevens worden verstrekt

## Artikel 24 Uitwisseling vanuit functie

1. In het kader van de functie van de medewerker kan er sprake zijn van overdracht van persoonsgegevens, bijvoorbeeld aan het Ministerie van Onderwijs, Cultuur en Wetenschappen en de Inspectie van het Onderwijs of bijvoorbeeld een vliegmaatschappij. Denk ook aan het verstrekken van het [Organisatie]-mailadres waar nodig als middel tot contact.

2. Dit privacyreglement is van toepassing op de uitwisseling zoals bedoeld in het eerste lid van dit artikel.

3. Daar waar geen andere wettelijke grondslag van toepassing is, wordt om toestemming gevraagd.

## Artikel 25 Overige derden

1. Persoonsgegevens worden op basis van wettelijke grondslagen in ieder geval verstrekt aan:

   - het UWV (o.a. bij ziekte);
   - de belastingdienst;
   - een gerechtsdeurwaarder in geval van loonbeslag;
   - de politie op vertoon van schriftelijk bevel.

2. Persoonsgegevens kunnen nader gespecificeerd aan derden, bijvoorbeeld aan hulpinstanties, worden verstrekt als [Organisatie] dit in het belang van de medewerker acht. Dit vindt pas plaats nadat het voornemen daartoe tijdig en op deugdelijke wijze aan de medewerker is bekendgemaakt en men in de gelegenheid is gesteld om toestemming te geven, dan wel bezwaar te maken zoals bedoeld in artikel 26 ‘Uit te oefenen rechten’ van dit reglement, voordat [Organisatie] de gegevens verstrekt.

# Hoofdstuk 7 Rechten van medewerkers

## Artikel 26 Uit te oefenen rechten

<u>Recht op inzage</u>

1. De medewerker heeft het recht te weten welke persoonsgegevens van hen worden verwerkt door [Organisatie]. De medewerker kan een verzoek indienen tot inzage. Dat kan gaan om zowel door de medewerker zelf verstrekte als vanuit andere bronnen toegevoegde persoonsgegevens.

2. [Organisatie] geeft de medewerker zo snel mogelijk, uiterlijk binnen vier weken na ontvangst van het verzoek tot inzage, inzage in de persoonsgegevens die worden verwerkt. Die inzage is kosteloos. Aan een verzoek om kopieën daarvan kunnen kosten worden verbonden.

3. Voordat een medewerker inzage krijgt in de persoonsgegevens, controleert [Organisatie] de identiteit van de medewerker. Een [Organisatie]-account of [Organisatie]-pas wordt in die situatie als geldig verificatiemiddel beschouwd. De medewerker die geen [Organisatie]-account of -pas heeft, wordt gevraagd het identiteitsbewijs te tonen. [Organisatie] gebruikt het identiteitsbewijs alleen ter verificatie van de identiteit van de medewerker. Er wordt geen kopie in de administratie opgeslagen voor dit proces.

Recht op correctie/rectificatie

1. Medewerkers hebben recht op verbetering, aanvulling of verwijdering van hun persoonsgegevens. Dat kan bijvoorbeeld aan de hand van een door de medewerker verstrekte verklaring. De rectificatie moet direct plaatsvinden.

2. [Organisatie] is verplicht iedere derde aan wie de persoonsgegevens zijn verstrekt in kennis te stellen van elke rectificatie en vragen deze door te voeren, tenzij dit onmogelijk is of onevenredig veel inspanning vraagt.

Recht op gegevenswissing (vergetelheid)

[Organisatie] is verplicht persoonsgegevens van de medewerker zonder onredelijke vertraging te wissen, onder andere als:

- persoonsgegevens niet langer nodig zijn voor de doeleinden waarvoor zij zijn verzameld;
- de medewerker de gegeven toestemming intrekt en er geen andere wettelijke grondslag is voor de verwerking;
- de persoonsgegevens onrechtmatig verwerkt zijn.

Het gaat hier om gegevens die door de medewerker zelf zijn verstrekt en die niet meer nodig zijn.

Recht op beperking van de verwerking

1. Medewerkers hebben het recht [Organisatie] te vragen hun gegevens (tijdelijk) niet te verwerken c.q. de verwerking (tijdelijk) op te schorten en/of te wijzigen als:

    - 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 medewerker bezwaar heeft gemaakt tegen de verwerking en in afwachting is van het antwoord op de vraag of de gerechtvaardigde gronden van [Organisatie] zwaarder wegen dan die van de medewerker.

2. [Organisatie] moet duidelijk aangeven dat de verwerking van de persoonsgegevens is beperkt, zodat dit ook duidelijk is voor andere partijen.

3. Als [Organisatie] de beperking wil opheffen dan moet [Organisatie] de medewerker hiervan voorafgaand op de hoogte brengen.

Recht op overdraagbaarheid van gegevens

1. Als aan alle voorwaarden voor uitoefening van het recht op gegevensoverdraagbaarheid is voldaan, heeft de medewerker het recht om de persoonsgegevens die men aan [Organisatie] heeft verstrekt en die digitaal zijn verwerkt, te ontvangen in een gestructureerde, gangbare

digitale vorm. Dit recht op dataportabiliteit is overigens primair bedoeld voor diensten die men zelf actief kiest en gebruikt, zoals sociale media, cloudopslag, muziekstreaming en is niet van toepassing op bijvoorbeeld systemen voor personeelsinformatie.a

2. De medewerker heeft het recht om de in lid 1 bedoelde gegevens aan een andere partij over te dragen. De medewerker kan vragen dit rechtstreeks van [Organisatie] naar de andere partij door te zenden als dit technisch mogelijk is.

Recht van bezwaar

1. Medewerkers kunnen bezwaar maken tegen de verwerking van hun persoonsgegevens.

2. Als de medewerker bezwaar maakt dan staakt [Organisatie] de verwerking van die persoonsgegevens, tenzij [Organisatie] dwingende gerechtvaardigde gronden aanvoert die zwaarder wegen dan de belangen, rechten en vrijheden van de medewerker.

## Artikel 27 Uitoefening rechten door medewerker

1. Voor de uitoefening van de rechten zoals genoemd in artikel 26 doet de medewerker een schriftelijk verzoek (bijvoorbeeld per e-mail) aan [het betreffende meldpunt]. De Privacy Officer beoordeelt het verzoek en zet het door naar de daartoe aangewezen personen binnen [Organisatie].

2. [Organisatie] bericht de medewerker zo spoedig mogelijk, uiterlijk binnen vier weken na ontvangst, over de afhandeling van het verzoek zoals bedoeld in lid 1 van dit artikel.

3. Als de medewerker het niet eens is met de behandeling van het ingediende verzoek, kan de deze daarover een klacht indienen. De medewerker stuurt een klacht rechtstreeks aan [de FG of een commissie voor klachtenafhandeling die de FG betrekt]. Als de klacht voor de medewerker niet tot een voor acceptabel resultaat leidt, kan deze zich wenden tot de Autoriteit Persoonsgegevens of de rechter.

## Artikel 28 Contactgegevens

1. De Privacy Officer is bereikbaar via privacy@[Organisatie].nl.

2. De Functionaris voor Gegevensbescherming is rechtstreeks bereikbaar via fg@[Organisatie].nl.

3. Autoriteit Persoonsgegevens, www.autoriteitspersoonsgegevens.nl, telefoonnummer (088) 180 52 50.