

## Gedragcode computerfaciliteiten en telefonie Nissewaard

Het college van burgemeester en wethouders van de gemeente Nissewaard;

- gelet op het gestelde in artikel 160 van de Gemeentewet waarbij de bevoegdheid tot het vaststellen, wijzigen en intrekken van de rechtspositieregelingen voor het gemeentelijk personeel en gewezen personeel wordt opgedragen aan het college;
- gelet op de Wet bescherming persoonsgegevens;
- gelet op gezien de brief van de ondernemingsraad van 26 mei 2016, waarin wordt ingestemd met het voorgenomen besluit tot vaststelling van de onderliggende regeling;

### besluit:

vast te stellen de volgende gedragcode computerfaciliteiten en telefonie Nissewaard:

### Hoofdstuk 1: Definities en werkingssfeer

#### Artikel 1 Definities

- a. Gebruiker: de ambtenaar volgens artikel 1:1 lid 1, sub a, van de CAR/UWO alsmede de persoon die (betaalde of niet-betaalde) werkzaamheden voor de gemeente verricht, anders dan in ambtelijk dienstverband die gebruik maken van de elektronische informatie- en communicatiesystemen
- b. Computerfaciliteiten: alle (ict) hulpmiddelen die worden gebruikt voor de geautomatiseerde informatievoorziening zoals apparatuur, programmatuur, netwerken, internet- en e-mail
- c. Decentrale netwerkfaciliteit: de op de buitenlocaties aanwezige en niet door Syntrophos centraal beheerde netwerkvoorzieningen, zoals de daar aanwezige Firewalls, routers, switchen en datalijnen.
- d. Centrale netwerkfaciliteit: de in de gemeentelijke gebouwen aanwezige en door Syntrophos centraal beheerde netwerkvoorzieningen, zoals de Firewalls, routers, switchen en datalijnen.
- e. Telefonie: vaste- en mobiele telefonie
- f. Extern toegang: toegang tot de centrale en decentrale netwerkfaciliteit van de gemeente vanuit een locatie anders dan een gemeentelijk gebouw
- g. Systeem: het geheel aan computerhardware, computersoftware en gegevensverzamelingen die beschikbaar en benaderbaar zijn via de centrale en decentrale netwerkfaciliteit
- h. Verantwoordelijke: het college; het bestuursorgaan dat het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt
- i. Systeembeheerder: degene die functioneel en technisch zorg draagt voor de elektronische informatiesystemen

#### Artikel 2 Werkingssfeer en eigendom

1. Deze gedragcode is van toepassing op een ieder die gebruik maakt van computerfaciliteiten en telefonie, ongeacht de locatie waar de werkzaamheden via het systeem of de centrale en decentrale netwerkfaciliteit worden verricht.
2. De computerfaciliteiten en telefonie zijn eigendom van, en worden ter beschikking gesteld door Syntrophos. Deze faciliteiten worden vervolgens beschikbaar gesteld aan de gebruiker door de gemeente Nissewaard.

### Hoofdstuk 2: Algemene regels en voorwaarden computerfaciliteiten en telefonie

#### Artikel 3 Gebruik computerfaciliteiten en telefonie

1. De aan de gebruiker ter beschikking gestelde computerfaciliteiten en telefonie zijn bedoeld voor zakelijk gebruik. Privégebruik wordt alleen toegestaan als dit de dagelijkse werkzaamheden niet negatief beïnvloedt en niet schadelijk is voor de (prestaties van) computerfaciliteiten en telefonie.
2. De gebruiker zal zorgvuldigheid betrachten bij het gebruik en het beheer van computerfaciliteiten en telefonie en de integriteit en goede naam van de gemeente waarborgen.

De gebruiker is verplicht zich te houden aan algemene instructies voor het gebruik van computerfaciliteiten en telefonie. Instructies en aanwijzingen die tijdens het gebruik van computerfaciliteiten worden gegeven moeten worden opgevolgd.

3. De gebruiker zal al wat redelijkerwijs van hem mag worden verlangd, doen om de vertrouwelijkheid, integriteit en beschikbaarheid van de gegevens die aanwezig zijn op de voor hem toegankelijke computerfaciliteiten en telefonie te waarborgen.

#### **Artikel 4 Ander gebruik**

1. De gebruiker dient zorgvuldig om te gaan met het installeren en gebruik van applicaties op de computerfaciliteiten.
2. Het is de gebruiker niet toegestaan de door de gemeente Nissewaard ter beschikking gestelde computerfaciliteiten en telefonie te kopiëren of ter beschikking te stellen aan derden.
3. De gebruiker zal geen acties ondernemen of pogingen hiertoe doen die de continuïteit of de beveiliging van de computerfaciliteiten en telefonie van de gemeente Nissewaard ondermijnen.

#### **Artikel 5 Toegang**

1. Toegang tot computerfaciliteiten wordt verleend op basis van een combinatie van gebruikersnaam en een persoonlijk wachtwoord of andere vergelijkbare identificatie- en authenticatiemiddelen.
2. Het is de gebruiker niet toegestaan zich ongeautoriseerd toegang te verschaffen tot gegevens van andere gebruikers of ongeautoriseerd programma's te gebruiken.
3. Voor het beheer van het persoonlijke wachtwoord gelden de volgende regels:
  - a. De gebruiker is verantwoordelijk voor het gebruik van de bevoegdheden, die aan de verstrekte gebruikersnaam zijn verbonden. De gebruiker moet alle redelijke maatregelen voor de beveiliging en geheimhouding van het wachtwoord hebben getroffen.
  - b. Het wachtwoord is strikt persoonlijk en niet overdraagbaar.
  - c. De gebruiker wijzigt bij de eerste de beste gelegenheid het aan hem verstrekte tijdelijke wachtwoord. Indien het niet mogelijk is dit wachtwoord te wijzigen, doet hij hiervan melding bij het Servicepunt.
  - d. Het opslaan van het wachtwoord en/of de combinatie gebruikersnaam/wachtwoord is niet toegestaan anders dan in hiervoor door de Syntrophos vrijgegeven programmatuur.
  - e. Ten aanzien van het wachtwoord is geheimhouding verplicht.
4. De gebruiker zal de in gebruik zijnde computerfaciliteiten en mobiele telefonie bij afwezigheid vergrendelen en het wachtwoordmechanisme bij reactivering moeten gebruiken.

#### **Artikel 6 Gebruik eigen apparatuur**

Voor het gebruik van apparatuur welke niet door de gemeente Nissewaard beschikbaar is gesteld gelden de volgende bepalingen:

- a. Een actueel anti-virusprogramma moet actief zijn op de apparatuur. Vereist is dat dit programma periodiek wordt geactualiseerd.  
Bij Windows-systemen dienen altijd de laatste updates te zijn geïnstalleerd.
- b. Voor Apple programmatuur is dit niet mogelijk. De gebruiker is bij het gebruik van Apple apparatuur verplicht om zijn programmatuur slechts te installeren vanuit de Apple App store.
- c. Het persoonlijk wachtwoord of andere vergelijkbare identificatie- en authenticatiemiddelen om verbinding te maken met de computerfaciliteiten en telefonie van de gemeente Nissewaard mag niet worden opgeslagen op de apparatuur, zodat automatisch kan worden ingelogd.

#### **Artikel 7 Melding incidenten**

1. Incidenten die het normale gebruik van de computerfaciliteiten verstoren, worden zo spoedig mogelijk gemeld via het Servicepunt. Hieronder vallen ook beveiligingsincidenten waar de gebruiker weet van heeft, maar niet zelf onmiddellijk hinder van heeft.
2. Wanneer de gebruiker een datalek in de zin van de Wet melding Datalekken constateert of vermoedt, dient hij hiervan onverwijld melding te maken via het servicepunt (telefonisch of via intranet).

### **Hoofdstuk 3: Extern toegang tot computerfaciliteiten**

#### **Artikel 8 Extern toegang tot computerfaciliteiten**

1. De gebruiker zal bij het gebruik van computerfaciliteiten waarbij extern toegang wordt gebruikt, zorgvuldig zijn bij het beheer en gebruik.
2. De gebruiker neemt maatregelen om te voorkomen dat derden informatie te zien krijgen, die niet voor hen bestemd is.
3. De gebruiker maakt geen gebruik van openbare gratis Wifi-netwerken op publiek terrein waar geen gebruik wordt gemaakt van wachtwoordauthenticatie.

### **Artikel 9 Geen externe toegang**

Voor door de gemeente Nissewaard, in het Beleid thuiswerkapplicaties, aangewezen applicaties geldt een verbod op het gebruik via externe toegang. Deze applicaties zijn niet toegankelijk via externe toegang. Indien deze applicaties na het inloggen toch voor de gebruiker beschikbaar zijn, dient de gebruiker dit terstond te melden via het Servicepunt. In ieder geval mag de betreffende applicatie niet worden opgestart.

## **Hoofdstuk 4 : Regels en voorwaarden voor het gebruik van e-mail en internet**

### **Artikel 10 Gebruik e-mail en internet**

1. Het gebruik van het aan de gebruiker op persoonlijke titel ter beschikking gestelde e-mailadres is strikt persoonlijk.
2. De gebruiker kan een e-mailbericht weigeren voor zover de betrouwbaarheid van dit bericht onvoldoende is gewaarborgd, gelet op de aard en de inhoud van het bericht en het doel waarvoor het wordt gebruikt.
3. Het is gebruiker niet toegestaan met behulp van de e-mailfaciliteiten kettingbrieven te versturen of pornografisch materiaal te versturen of op te vragen, dan wel aanstootgevende, dreigende, lasterlijke, seksueel intimiderende, onzedelijke, racistische of discriminerende opmerkingen te maken.
4. Het is gebruiker niet toegestaan met behulp van de e-mailfaciliteiten illegale software te verzenden of op te vragen dan wel bestanden zonder voorafgaand overleg met de systeembeheerder(s) te verzenden of op te vragen waarvan de gebruiker redelijkerwijs moet aannemen dat deze te omvangrijk of vertrouwelijk van aard zijn.
5. Het is gebruiker niet toegestaan met behulp van de internetfaciliteiten bewust internetsites te bezoeken die pornografisch, dan wel racistisch materiaal bevatten of die naar algemeen maatschappelijke maatstaven als lasterlijk, beledigend, aanstootgevend, onzedelijk of oneerlijk worden beschouwd, mee te doen in chat-sessies, on line te gokken, illegale software te downloaden, dan wel zonder voorafgaand overleg met de systeembeheerder(s) bestanden te downloaden waarvan gebruiker redelijkerwijs moet aannemen dat deze te omvangrijk of schadelijk voor de computerfaciliteiten en telefonie en/of bedrijfsvoering kunnen zijn.
6. Zonder voorafgaande toestemming van de systeembeheerder(s) is het gebruiker niet toegestaan met behulp van de e-mailfaciliteiten een elektronisch bericht aan alle of vrijwel alle gebruikers van de gemeente tegelijkertijd te versturen.
7. Indien gebruiker met gebruik van de internetfaciliteiten handelingen verricht die als e-mailtoepassingen zijn te kwalificeren, dan zijn de bepalingen van artikel 10, derde en vierde lid, van overeenkomstige toepassing.

### **Artikel 11 Social Media**

1. Woordvoering met de pers op grond van berichten in de social media vindt in het algemeen plaats door de medewerkers van de afdeling Communicatie van de gemeente Nissewaard.
2. Wanneer een gebruiker uit hoofde van zijn functie gebruik maakt van social media, maakt hij zichzelf kenbaar met naam en functie. Alleen die informatie mag verstrekt worden waartoe men bevoegd is.
3. De gebruiker mag bij deelname aan social media als privépersoon geen mededelingen doen namens de gemeente Nissewaard, maar moet aangegeven dat meningen op persoonlijke titel worden geuit.

### **Artikel 12 Beveiliging**

Wanneer de beveiliging of de continuïteit van het e-mailgebruik dit vereist, is de verantwoordelijke gerechtigd voor gebruikers bestemde e-mailberichten te lezen, kopiëren, te vernietigen of bijlagen te verwijderen.

## **Hoofdstuk 5: Controle, bewaring en verwijdering persoonsgegevens**

### **Artikel 13 Algemeen**

Dit hoofdstuk is van toepassing op het verwerken van persoonsgegevens inzake het gebruik van computerfaciliteiten en telefonie. Het geeft de wijze aan waarop in de gemeente wordt omgegaan met computerfaciliteiten en telefonie en omvat regels ten aanzien van verantwoord gebruik hiervan en regels over de wijze waarop controle hiervan plaatsvindt.

### **Artikel 14 Doeleinden**

De verwerking van persoonsgegevens van gebruikers inzake het gebruik van computerfaciliteiten en telefonie heeft de volgende doeleinden:

- a. het verkrijgen van inzicht in de mate van gebruik van computerfaciliteiten en telefonie;
- b. het voorkomen van dan wel constateren van onrechtmatig gebruik dan wel misbruik van computerfaciliteiten en telefonie;
- c. het beveiligen van het systeem en het netwerk.

#### **Artikel 15 Controle algemeen**

1. Controle door verantwoordelijke op het gebruik van de computerfaciliteiten en telefonie vindt slechts plaats in het kader van de in artikel 14 genoemde doeleinden. Deze doeleinden stellen beperkingen aan de omvang en wijze van controle.
2. Controle ter verkrijging van inzicht in de mate van gebruik van de computerfaciliteiten en telefonie wordt beperkt tot de verkeersgegevens (tijd, hoeveelheid, omvang en dergelijke).
3. Controle ter voorkoming van onrechtmatig gebruik dan wel misbruik van de computerfaciliteiten en telefonie wordt zo beperkt mogelijk gehouden, in die zin dat deze in redelijke verhouding staat tot het doel waarvoor deze wordt aangewend. Bovendien vindt de controle in beginsel geanonimiseerd en slechts steekproefsgewijs plaats.
4. Controle in het kader van het beveiligen van het systeem en het netwerk voor het tegengaan van virussen en andere schadelijke programma's vindt op geautomatiseerde wijze plaats.
5. De controlebeperkingen, die in deze gedragscode worden opgelegd gelden niet voor die systemen waarvoor andere (wettelijk) voorgeschreven normen bestaan.  
Indien dit het geval is worden gebruikers van die systemen daar separaat over ingelicht.

#### **Artikel 16 Wijze van controle**

1. Controle vindt in beginsel plaats op het niveau van getotaliseerde gegevens die niet herleidbaar zijn tot individuele personen. Controle ter verkrijging van inzicht in de mate van het gebruik van de computerfaciliteiten en telefonie kan echter ook op gebruikersniveau plaatsvinden. Indien een gebruiker of een groep gebruikers wordt verdacht van het overtreden van regels, kan gedurende een vastgestelde (korte) periode gerichte controle op de inhoud plaatsvinden.
2. Controle beperkt zich in principe tot verkeersgegevens van het gebruik van de computerfaciliteiten en telefonie.
3. Bij zwaarwegende redenen, aanvullend op het reeds genoemde in lid 1, vindt er, met uitzondering van de categorie telefonie, controle op de inhoud plaats.

#### **Artikel 17 Controle op inhoud**

1. De controle op de inhoud vindt plaats naar aanleiding van gerechtvaardigde vermoedens dan wel constatering van onjuist gebruik als bedoeld in de artikelen van dit reglement.  
Gericht onderzoek heeft als hoofddoelen:
  - a. het vaststellen van oneigenlijk gebruik van computerfaciliteiten en telefonie;
  - b. het controleren van gemaakte afspraken over het (verboden) gebruik;
  - c. het controleren of de inhoud voldoende wordt beschermd en niet openbaar wordt of is gemaakt.
  - d. het voorkomen van negatieve publiciteit over de gemeente Nissewaard.
2. De gebruiker wordt schriftelijk geïnformeerd over de resultaten van het onderzoek. Indien het onderzoek geen aanleiding geeft tot verdere maatregelen wordt het schriftelijk verslag vernietigd.

#### **Artikel 19 Controle gebruikers**

1. De controle op de inhoud vindt plaats na schriftelijke opdracht van de leidinggevende of van de CISO aan de systeembeheerder en wordt uitgevoerd door een daartoe aangewezen persoon. In de opdracht van de leidinggevende wordt vermeld waarom het onderzoek plaatsvindt en waarom – voor zover dit aan de orde is – de gebruiker pas achteraf van het onderzoek op de hoogte wordt gesteld. Indien geconstateerd wordt dat een gebruiker deze gedragscode overtreedt, dan wordt de betrokken gebruiker zo spoedig mogelijk hierop aangesproken door de leidinggevende.
2. Voordat de leidinggevende de schriftelijke opdracht aan de systeembeheerder verstrekt, legt hij de opdracht ter instemming voor aan de gemeentesecretaris.
3. Het gebruik van de computerfaciliteiten en telefonie door leden van de ondernemingsraad, leden van het Georganiseerd Overleg, bedrijfsartsen en andere medewerkers met een vertrouwensfunctie zijn in beginsel uitgesloten van controle.  
Dit geldt niet voor de controle op de veiligheid van het elektronische verkeer.

#### **Artikel 20 Bewaring en verwijdering**

1. Persoonsgegevens, gerelateerd aan de computerfaciliteiten en telefonie, worden maximaal zes maanden bewaard. Gegevens die ouder zijn dan zes maanden worden automatisch verwijderd, tenzij er bijzondere redenen zijn, bijvoorbeeld een zwaarwegend vermoeden van onrechtmatig

gebruik dan wel misbruik van de computerfaciliteiten en telefonie, om de gegevens langer te bewaren. Dat moet dan expliciet kunnen worden gemaakt en worden gemeld aan het Autoriteit persoonsgegevens.

2. Indien de systeembeheerder om technische redenen persoonsgegevens, gerelateerd aan de computerfaciliteiten en telefonie, niet kan verwijderen na afloop van de periode van 6 maanden, wordt onder verwijderen verstaan het niet meer verstrekken van deze gegevens voor de in artikel 14 geformuleerde doeleinden.

## **Hoofdstuk 6: Rechten van gebruiker: verbeteren, aanvullen, verwijderen of afschermen persoonsgegevens**

### **Artikel 21 Rechten van de gebruiker**

1. Aan de gebruiker die daarom aan verantwoordelijke verzoekt wordt een overzicht verschaft van de hem betreffende persoonsgegevens die worden verwerkt.
2. De gebruiker kan de verantwoordelijke verzoeken zijn persoonsgegevens te verbeteren, aan te vullen, te verwijderen of af te schermen. Dit indien deze feitelijk onjuist zijn, voor het doel of de doeleinden van de verwerking onvolledig of niet ter zake dienend zijn dan wel anderszins in strijd met een wettelijk voorschrift worden verwerkt.
3. De verantwoordelijke bericht de verzoeker binnen vier weken na ontvangst van het in het tweede lid genoemde verzoek schriftelijk of, dan wel in hoeverre, hij daaraan voldoet. Een weigering is met redenen omkleed. Een beslissing op een verzoek geldt als een besluit in de zin van artikel 1:3, Algemene wet bestuursrecht.
4. De verantwoordelijke draagt er zorg voor dat een beslissing tot verbetering, aanvulling, verwijdering of afscherming zo spoedig mogelijk wordt uitgevoerd.

## **Hoofdstuk 7: Sancties, schade, onvoorzien, openbaarmaking, evaluatie en Wet bescherming persoonsgegevens**

### **Artikel 22 Sancties**

1. Overtreding van deze gedragscode kan voor werknemers in dienst van de gemeente Nissewaard resulteren in disciplinaire maatregelen of ontslag als disciplinaire straf als bedoeld in de Collectieve Arbeidsvoorwaardenregeling van de gemeente.
2. Overtreding van deze gedragscode kan voor personen die (betaalde of niet-betaalde) werkzaamheden voor de gemeente verrichten, anders dan in ambtelijk dienstverband, resulteren in:
  - a. maatregelen waardoor deze personen, al dan niet tijdelijk, geen beschikking meer hebben over (een deel van) de elektronische communicatiemiddelen;
  - b. maatregelen die leiden tot ontbinding van de overeenkomst die de grondslag vormt voor het verrichten van werkzaamheden bij de gemeente.
3. Bij strafbare feiten kan door of vanwege de gemeente aangifte worden gedaan.

### **Artikel 23 Schade**

Schade die is ontstaan doordat een gebruiker in strijd met deze gedragscode heeft gehandeld, zal door de verantwoordelijke op die gebruiker worden verhaald.

### **Artikel 24 Onvoorzien**

Voor gebruikers geldt dat in gevallen waarin deze gedragscode niet voorziet of bij twijfel over de toepassing ervan, het college beslist.

### **Artikel 25 Openbaarmaking**

Deze gedragscode wordt verstrekt of ter beschikking gesteld aan alle gebruikers die, direct of indirect, de beschikking krijgen over computerfaciliteiten en telefonie.

### **Artikel 26 Wet bescherming persoonsgegevens**

Onverminderd het bepaalde in deze gedragscode, zal op het verwerken van persoonsgegevens de Wet bescherming persoonsgegevens van toepassing zijn.

## **Hoofdstuk 8: Slotbepalingen**

### **Artikel 27 Intrekking oude regeling**

1. Het 'Privacyreglement elektronische communicatiemiddelen Nissewaard' blijft voor politieke ambtsdragers van kracht tot de nieuwe gedragscode voor hen van kracht is.

2. Het 'Privacyreglement elektronische communicatiemiddelen Nissewaard' is vanaf de dag na die van de inwerkingtreding van de nieuwe gedragscode niet meer van toepassing op de in artikel 1 sub a omschreven gebruiker.

### **Artikel 28 Inwerkingtreding**

Deze regeling treedt in werking op de dag na bekendmaking.

### **Artikel 29 Citeertitel**

Deze regeling wordt aangehaald als: Gedragscode computerfaciliteiten en telefonie Nissewaard.

*Aldus vastgesteld door het college van de gemeente Nissewaard van 12 april 2016,*

*De gemeente secretaris,  
M.L.M. Weerts*

*de burgemeester,  
M. Salet*

## **Toelichtingen:**

### **Artikel 6 sub c:**

Als gebruiker dien je altijd een persoonlijk wachtwoord of andere vergelijkbare beveiligings-maatregelen op de apparatuur in te stellen, zodat bij bijvoorbeeld onbeheerd laten, verlies of diefstal van je eigen apparatuur de kans beperkt wordt dat anderen automatisch kunnen inloggen.

### **Artikel 7, lid 2:**

#### **Datalek**

Bij een datalek gaat het om toegang tot of vernietiging, wijziging of vrijkomen van persoonsgegevens bij een organisatie zonder dat dit de bedoeling is van deze organisatie. Onder een datalek valt dus niet alleen het vrijkomen (leken) van gegevens, maar ook onrechtmatige verwerking van gegevens. We spreken van een datalek als er een inbreuk is op de beveiliging van persoonsgegevens (zoals bedoeld in artikel 13 van de Wet bescherming persoonsgegevens). Bij een datalek zijn de persoonsgegevens blootgesteld aan verlies of onrechtmatige verwerking – dus aan datgene waartegen de beveiligingsmaatregelen bescherming moeten bieden.

Voorbeelden van datalekken zijn: een kwijtgeraakte USB-stick met persoonsgegevens, een gestolen laptop of een inbraak in een databestand door een hacker.

### **Artikel 8 lid 3:**

Netwerken waarbij je geen code hoeft in te geven om toegang te krijgen tot een netwerk zijn altijd verdacht. Ook wanneer de gebruiker akkoord moet gaan met een reglement of zo. Het is niet zo dat de leverancier van dit netwerk kwaads in de zin heeft. Iedereen heeft vrij toegang tot dat netwerk en kan doen en laten wat hij wil. Dit betekent dus dat een dergelijk netwerk nooit vertrouwd kan worden. Bij dergelijke netwerken verdient het altijd aanbeveling gebruikt te maken van je eigen 4G voorziening of een netwerk waartoe je door middel van een unieke login-naam wachtwoordcombinatie, zodat alle gebruikers van dat netwerk op enigerlei wijze geïdentificeerd kunnen worden. De werkomgeving van de portal Syntrophos is beveiligd en daarbinnen kan de gebruiker er vanuit gaan dat hij veilig werkt.

### **Artikel 9:**

De applicaties, die niet via een externe toegang gebruikt mogen worden, worden vastgelegd in het Beleid thuiswerkapplicaties.

### **Artikel 10 lid 4:**

De gebruiker dient bij omvangrijke e-mailbestanden met of zonder vreemde extensies bij zich zelf ten rade gaan of het verstandig is om de e-mail en/of bijlage te openen, door testuren of op te slaan. Wat omvangrijk of vreemd kan zijn, wordt door de werkgever duidelijk aangegeven.

### **Artikel 20, lid 1**

De bewaartermijn van 6 maanden is wettelijk bepaald.

### **Artikel 22**

Bij het opleggen van een disciplinaire maatregel geldt voor de werknemer op grond van de Algemene wet bestuursrecht het recht op hoor en wederhoor. Daarnaast heeft de werknemer hiermee ook de mogelijkheid tot bezwaar en beroep.