Artikelsgewijze Toelichting

Considerans

In de considerans staat ondermeer de datum waarop de GO en de OR van de diensten instemming met het privacyreglement heeft gegeven.

Artikel 1 Definities

De begrippen zoals die in het privacyreglement voorkomen worden hier gedefinieerd. Voor de omschrijving van begrippen is waar mogelijk aangesloten bij de bewoording die wordt gebruikt in de WBP.

De WBP is van toepassing als er sprake is van verwerking van persoonsgegevens. Gegevens met betrekking tot het e-mail- en internetgebruik van medewerkers zijn in het algemeen te kwalificeren als persoonsgegevens. IP-adressen zijn in combinatie met de username en het password te herleiden tot een bepaalde gebruiker. De daaraan verbonden bestanden zijn aldus herleidbaar tot een medewerker. De verkeersgegevens geven inzicht in de afzender, de bestemming, de datum en de tijd van het bericht of van het internetgebruik. Ook de inhoud van het e-mailbericht is een persoonsgegeven als de werkgever dit tot zijn beschikking heeft om bijvoorbeeld te controleren of een medewerker de regels in het privacyreglement nakomt. De WBP hanteert een ruime definitie voor het begrip 'verwerking': het gehele proces van verzamelen tot aan vernietigen van gegevens.

Ten behoeve van de gemeente Groningen zijn definities toegevoegd voor de begrippen: e-mailberichten, functionele of zakelijke e-mail, formele e-mail en informele email. Het onderscheid dat gemaakt wordt tussen formele en informele e-mail heeft tot doel adequaat formele berichtenstromen te identificeren en juist te archiveren.

Artikel 2 Reikwijdte

Het privacyreglement is van toepassing op het verwerken van persoonsgegevens inzake het gebruik van e-mail en/of internetfaciliteiten.
Het privacyreglement geldt voor alle medewerkers van de gemeente Groningen: ambtenaren en personen die (betaald of niet-betaald) werkzaamheden voor de gemeente verrichten, anders dan in ambtelijk dienstverband

Bestuurders

Het privacyreglement is (in deze vorm) dus niet van toepassing op politieke ambtsdragers. De VNG zal het echter zodanig aanpassen, dat ook een privacyreglement voor bestuurders wordt ontwikkeld. Dit zou in de eerste helft van 2005 aan de gemeenten worden gestuurd. Begin 2006 is de status hiervan nog steeds onbekend.

Artikel 3 Doeleinden

De WBP bepaalt dat gegevens in overeenstemming met de wet en op een behoorlijke en zorgvuldige wijze moeten worden verwerkt (artikel 6 WBP). Dit voorschrift geldt in zoverre als de privacyrechtelijke evenknie van de arbeidsrechtelijke norm van goed werkgeverschap. Persoonsgegevens mogen voorts slechts voor welbepaalde, duidelijk omschreven en gerechtvaardigde doeleinden worden verwerkt (artikel 7 WBP). Deze doelomschrijving moet nauwkeurig en zo volledig mogelijk zijn (zie ook artikel 4, eerste lid privacyreglement).

In overleg moet worden vastgesteld welke doeleinden voor controle van e-mail- en internetgebruik noodzakelijk zijn voor de eigen organisatie. Controle via volgsystemen is dus alleen toegestaan indien het doel van de controle vooraf is bepaald. Als grondslag van de controle kan doorgaans het gerechtvaardigd belang van de organisatie worden aangewezen (artikel 8, onder sub f WBP). De privacybelangen van de medewerkers horen hierbij dan wel meegewogen te worden. De aard, omvang en vorm van de controlemaatregelen dienen dus in een redelijke verhouding tot het doel van de controle te staan (proportionaliteit), (zie ook artikel 6, eerste lid, onder sub b en de toelichting). Tevens geldt dat de gebruikte controlemiddelen niet meer inbreuk mogen maken op de belangen van de medewerker dan strikt noodzakelijk is (subsidiariteit). In het privacyreglement zijn zes doeleinden geformuleerd.

Leden d, e en f zijn aanvullend voor de gemeente Groningen opgenomen. Hiertoe is ook artikel 6 'Controle' aangevuld. Het betreft hier:

a. begeleiding en/of individuele beoordelingen;
b. bewijs en archivering;
c. bescherming van onder geheimhouding vallende of niet-openbare informatie.

Controle van e-mail en controle op het internetgebruik is dus op zichzelf niet verboden. De werkgever is bevoegd om op basis van zijn gezagsbevoegdheid voorwaarden te stellen aan het gebruik van e-mail- en internetfaciliteiten of bepaalde soorten gebruik te verbieden. De werkgever moet wel de doeleinden bepalen waarvoor hij controle noodzakelijk acht (doelbinding).

Artikel 4 Verantwoordelijkheden en beheer

Artikel 4, eerste lid

Op de werkgever wordt geen absolute verplichting gelegd. Een garantie voor de juistheid van gegevens kan van de werkgever niet worden gevergd. De juistheid van de gegevens wordt mede bepaald door de context waarin ze worden gebruikt. Met 'nodige' maatregelen wordt uitgedrukt dat alle maatregelen moeten worden getroffen die in redelijkheid kunnen worden gevergd. De redelijkheid stelt daarbij, afhankelijk van bijvoorbeeld de soort gegevens die onderwerp van verwerking zijn, de stand van de techniek en de kosten die met de maatregelen gepaard gaan, grenzen aan de te nemen maatregelen.

Artikel 4, tweede lid

Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van te beschermen gegevens met zich meebrengen. De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen.

Artikel 4, derde lid

Een of meer systeembeheerders zijn met het beheer van de bestanden belast. De systeembeheerder heeft uit hoofde van zijn functie toegang tot alle gegevens in het computernetwerk. De functie van systeembeheerder dient met de nodige waarborgen te worden omgeven. De systeembeheerder moet zich ervan bewust zijn dat hij gegevens die hij tijdens zijn werk tegenkomt, geheim dient te houden. Die verplichting lijdt uitzondering indien enig wettelijk voorschrift hem tot mededeling verplicht of uit zijn taak de noodzaak tot mededeling voortvloeit. De systeembeheerder is uiteraard in beginsel niet bevoegd tot het lezen van documenten of e-mail of het meekijken met het internetgebruik van de medewerkers zonder dat daar een bijzondere aanleiding voor is.

De systeembeheerder dient tegenover het management een zekere onafhankelijkheid te hebben. Er moet dus een heldere procedure te bestaan over wie in welke gevallen de systeembeheerder opdracht kan geven om bepaalde zaken op het netwerk nader te controleren of daarover informatie te verschaffen.

Back-ups

In het kader van zorgvuldigheid zullen regelmatig back-ups van de systemen worden gemaakt die in geval van calamiteiten eenvoudig kunnen worden teruggezet. Dit betekent dat van logbestanden en andere gegevens over het e-mail- en internetgedrag van medewerkers een back-up wordt gemaakt. De werkgever moet zich ervan bewust zijn dat onzorgvuldig of onbevoegd gebruik van deze back-ups even schadelijk kan zijn voor de persoonlijke levenssfeer van de medewerker als onzorgvuldig of onbevoegd gebruik van het actuele systeem. Back-ups dienen daarom op een veilige plaats bewaard te worden. Nadat gegevens zijn aangepast moet zo snel mogelijk een nieuwe back-up gemaakt worden en moeten oude versies worden vernietigd, zodat de gegevens niet na een eventuele terugplaatsing van een back-up nogmaals moeten worden aangepast.

Artikel 5 Gebruik elektronische communicatiemiddelen

In het privacyreglement worden gedragsregels opgenomen over wat er in de organisatie onder verantwoord e-mail- en internetgebruik wordt verstaan.

In het privacyreglement worden bovendien regels opgenomen over wat niet is toegestaan bij een verantwoord e-mail- of internetgebruik.

Artikel 5 van het VNG model is voor de gemeente Groningen uitgebreid met de leden 8. tot en met 14. Deze leden geven meer gerichte aanwijzigen ten aanzien van het gebruik van e-mail en internet.
Zo zal uitgaande e-mail worden voorzien van een automatisch toegevoegde disclaimer zodra dit technisch realiseerbaar is(lid 9). Alle uitgaande e-mail wordt hiermee herkenbaar als zijnde afkomstig van de gemeente Groningen. De disclaimer beschermt tevens, in beperkte mate, tegen aansprakelijkheid.
Een belangrijk element wordt gevormd door de in lid 10 opgenomen statusaanduiding van e-mail. Wat kan wel en wat niet geregeld worden per e-mail in het dagelijks werk. Ondanks de mogelijkheid e-mail dezelfde juridische status als bijvoorbeeld een ingekomen of uitgaande brief te geven, zijn hiertoe de technische voorzieningen nog niet geïmplementeerd. Door de implementatie van voorzieningen voor authenticatie (elektronische handtekening, DigiD) en een adequate archivering van e-mail in een digitaal documentmanagementsysteem op kortere termijn, mag verwacht worden dat de status van e-mail zal veranderen.

Het aangaan van (financiële) verplichtingen is per e-mail niet toegestaan (lid 11), tenzij hiervoor toestemming is gekregen.

Om de goede werking van het netwerk en de PC's te kunnen garanderen zijn beperkingen gesteld aan het opvragen, versturen, installeren en uitvoeren van bestanden en programma's (leden 12, 13 en 14). Ook het voorkomen van het binnenhalen van virussen en spam wordt door deze leden beoogd naast de technische en softwarematige voorzieningen die de organisatie al inzet.

Een totaal verbod van privé-gebruik van de elektronische communicatiemiddelen is overigens niet mogelijk. Er is een duidelijke uitspraak gedaan over de huidige 'privétisering' van de werkplek. Dat houdt in dat een bepaalde mate van niet-zakelijk e-mail- en internetgebruik onder werktijd niet kan worden verboden.

(Kantonrechter Haarlem, 16 juni 2000, Jurisprudentie Arbeidsrecht 2000, 170). De werkgever kan wel beperkende voorwaarden opstellen aan het persoonlijk gebruik van de elektronische communicatiemiddelen.

Artikel 6 Controle

Artikel 6, eerste lid, onder sub a

Voor het verkrijgen van inzicht in de mate van gebruik van de elektronische communicatiemiddelen zal in het kader van kosten- en capaciteitsbeheersing de controle beperkt kunnen blijven tot verkeersgegevens. Kennisneming van de inhoud is dan niet noodzakelijk.

Het is echter ook mogelijk dat u inzicht wilt hebben in de meest bezochte internetsites, bijvoorbeeld in de vorm van een top tien. Daarvoor zal wel kennisgenomen dienen te worden van inhoudelijke gegevens. Indien dit wenselijk is, dan dient u het eerste lid, onder sub a, aan te passen.

Artikel 6, eerste lid, onder sub b

Bovendien vindt de controle in beginsel geanonimiseerd en slechts steekproefsgewijs plaats.

De genomen maatregelen dienen in redelijke verhouding te staan tot de belangen van de medewerker en de gebruikte middelen mogen niet een verdergaande inbreuk maken op die belangen dan strikt noodzakelijk is (proportionaliteit en subsidiariteit). Steeds zal hiertoe een belangenafweging moeten plaatsvinden. Het doel rechtvaardigt dus niet een continue controle en de daarmee gepaard gaande verregaande inbreuk op de persoonlijke levenssfeer van de werknemer. In beginsel zal de controle op naleving slechts steekproefsgewijs mogen geschieden.

Content filtering
Het is betrekkelijk eenvoudig om de datapakketjes die de server passeren te screenen op inhoud (content filtering). Dit houdt in dat geautomatiseerd wordt gekeken of bestanden woorden of teksten bevatten die de werkgever heeft verboden. Ook kan worden gekeken of de extensie is toegestaan. Indien bestanden worden gevonden die voldoen aan de zoektermen, zal door het systeem 'alarm' geslagen worden. De bestanden kunnen worden tegengehouden, teruggestuurd, apart gezet, gekopieerd, gelogd, etc.

Content filtering kan de communicatievrijheid en de persoonlijke levenssfeer van de gebruiker aantasten. Voor het gebruik ervan zal de werkgever een gerechtvaardigd belang moeten hebben. Ook zal het moeten voldoen aan de eisen van proportionaliteit en subsidiariteit. Dit betekent dat onder meer zal moeten worden bezien in hoeverre content filtering noodzakelijk is, welke zoektermen worden gebruikt, welke actie wordt ondernomen nadat een 'hit' is gevonden, en welke procedures er bestaan om gerechtvaardigd gebruik van aangewezen zoektermen mogelijk te maken.
Content filtering kan dus alleen worden ingezet als de zoektermen vanuit het belang van de gemeente gerechtvaardigd zijn en ook zo nauwkeurig zijn dat gerechtvaardigd gebruik zo veel mogelijk ongemoeid wordt gelaten. Mits het met de nodige zorgvuldigheid wordt ingezet, zal content filtering als controlemiddel in mindere mate inbreuk maken op de privacy en de communicatievrijheid van de gebruiker dan andere vormen van controle, zoals volledige inhoudscontrole of steekproefsgewijze inhoudscontrole. Met behulp van content filtering zal verboden gebruik waarbij berichten worden opgesteld in codetaal of met versleuteling, niet kunnen worden opgespoord.

Bij het gebruik van content filtering kunnen dus, afhankelijk van de wijze waarop het wordt toegepast, veel of weinig persoonsgegevens worden verwerkt. Het kan worden ingezet om onrechtmatig gebruik en misbruik van de elektronische communicatiemiddelen automatisch te blokkeren of te retourneren. In dat geval hoeven er geen persoonsgegevens te worden gerapporteerd (zie artikel 6, vierde lid, en de toelichting). Tevens kan met behulp van content filtering op persoonsniveau rapportages worden gemaakt van onrechtmatig gebruik dan wel misbruik van de elektronische communicatiemiddelen. In het geval dat content filtering wordt ingezet voor controle van onrechtmatig gebruik dan wel misbruik van de elektronische communicatiemiddelen, dient dit in beginsel geanonimiseerd plaats te vinden.

Artikel 6, eerste lid, onder sub c
Onder sub c is opgenomen:

c. *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;*

Vanuit beveiligingsoogpunt is het wenselijk om e-mail- en internetgebruik te controleren. Het kan dan gaan om het tegengaan van systeemaanvallen door virussen, trojans of andere schadelijke programma's.

Bij deze controle verdient een geheel geautomatiseerde controle van de inkomende berichten (inclusief bijlagen) de voorkeur. Indien een besmet bericht gevonden wordt, kan dit op een aparte locatie worden bewaard voor nader onderzoek en eventuele herstelwerkzaamheden. Uiteraard wordt hierbij geen onderscheid gemaakt in zakelijke en privé-mail.

Ook een geheel geautomatiseerde controle van de inkomende internetcontent verdient voor dit doel de voorkeur. Indien het voor de inhoud van de functie van de medewerkers niet noodzakelijk is dat zij steeds toegang hebben tot internet, kan dit doel eenvoudig bereikt worden door de toegang aan te bieden op aparte computers die niet aan het interne netwerk zijn verbonden.

Artikel 6, eerste lid, onder sub d
Indien in artikel 3 meer doeleinden worden ingevuld (zie artikel 3, toelichting), dient artikel 6, eerste lid ook te worden uitgebreid met de controle op deze doeleinden. De controle zou bij de voorbeelddoeleinden als volgt kunnen worden beschreven.

- *begeleiding en/of individuele beoordelingen: in het kader van begeleiding en/of individuele beoordelingen vindt er steekproefsgewijs controle plaats van zakelijke e-mailberichten zoals overeengekomen met de individuele medewerker;*
- *bewijs en archivering: conform de regels maakt (nader in vullen) een kopie van de zakelijke e-mailberichten met als doel bewijs en/of archivering;*
- *bescherming van onder geheimhouding vallende of niet-openbare informatie: controle op het openbaar maken c.q. laten uitlekken van deze informatie vindt plaats op basis van steekproefsgewijze content filtering. Een verdacht bericht wordt apart gezet voor nader onderzoek. Onderscheid tussen privé- en zakelijk e-mail is niet van belang.*

De hierboven genoemde suggesties zijn in het privacyreglement voor de gemeente Groningen opgevolgd en toegevoegd.

Artikel 6, tweede lid
In het tweede lid is opgenomen:

2. *Controle vindt in beginsel plaats op het niveau van getotaliseerde gegevens die niet herleidbaar zijn tot individuele personen. Indien een medewerker of een groep medewerkers wordt verdacht van het overtreden van regels, kan gedurende een vastgestelde (korte) periode gerichte controle plaatsvinden.*

Het is in het algemeen niet noodzakelijk om het management rapportages en gebruiksstatistieken van het e-mail- en internetgebruik van de medewerkers op persoonsniveau te verstrekken. De gegevens in de rapportages en statistieken zullen dus meestal ontdaan kunnen worden van hun identificerende kenmerken. Alleen als er concrete bedenkingen bestaan tegen een bepaalde medewerker, is rapportage op persoonsniveau noodzakelijk en dan ook toegestaan.

Artikel 6, derde lid
In het derde lid is opgenomen:

3. *Controle beperkt zich in principe tot verkeersgegevens van het gebruik van de elektronische communicatiemiddelen. Alleen bij zwaarwegende redenen vindt er controle op de inhoud plaats.*

In principe is de controle van de elektronische communicatiemiddelen beperkt tot de verkeersgegevens. Dit zijn gegevens met betrekking tot datum, tijd, hoeveelheid en omvang. Slechts bij *zwaarwegende* redenen wordt er inhoudelijk gecontroleerd.

Artikel 6, vierde lid
Onrechtmatig gebruik dan wel misbruik van de elektronische communicatiemiddelen kan worden ingebouwd in de software die wordt gebruikt om te e-mailen of te internetten. Vaak zal dit kunnen door content filtering (scannen van berichten of bestanden op verboden woorden, extensies, beeldmateriaal), door het afsluiten van websites of nieuwsgroepen, het stoppen van de doorgifte, etc. Overtreding van het privacyreglement wordt hiervoor dan feitelijk vrijwel onmogelijk gemaakt en er is geen grond meer voor actieve controle en logging op het gebruik van de elektronische communicatiemiddelen.
Ook is het mogelijk om toepassingen volledig af te sluiten door de daarvoor benodigde software zelf niet aan te bieden.

Content filtering
Zie voor meer informatie over content filtering de toelichting bij artikel 6, eerste lid, onder b.
Daar komt ook aan de orde dat content filtering op verschillende wijzen kan worden ingezet.
- Content filtering om onrechtmatig gebruik dan wel misbruik van de elektronische communicatiemiddelen automatisch te blokkeren, of te retourneren (artikel 6, vierde lid). In dat geval hoeven er geen persoonsgegevens te worden gerapporteerd.
- Content filtering om op persoonsniveau rapportages van onrechtmatig gebruik dan wel misbruik van de elektronische communicatiemiddelen te maken (artikel 6, eerste lid, onder b). In het geval dat content filtering wordt gebruikt voor controle van onrechtmatig gebruik dan wel misbruik van de elektronische communicatiemiddelen dient dit in beginsel geanonimiseerd plaats te vinden.

Artikel 6, vijfde lid

5. *Indien geconstateerd wordt dat een medewerker dit privacyreglement overtreedt, dan wordt de betrokken medewerker zo spoedig mogelijk hierop aangesproken door de algemeen directeur.*

Een bepaalde tijd voor opbouw van het dossier is toegestaan indien de omstandigheden daartoe aanleiding geven. Indien de medewerker op zijn handelen in strijd met het privacyreglement wordt aangesproken, is het raadzaam dat hij gewaarschuwd wordt voor de (rechtspositionele) gevolgen bij continuering van dit gedrag. De algemeen directeur spreekt de medewerker op zijn gedrag aan.

Artikel 6, zesde lid

6. *Het gebruik van de elektronische communicatiemiddelen door OR-leden, GO-leden, 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.*

Deze bepaling betreft allereerst de communicatie per e-mail van leden van de OR ten behoeve van hun OR-werkzaamheden. Op grond van artikel 17 Wet Ondernemingsraden (WOR) hebben zij het recht om onderling te overleggen met gebruik van voorzieningen waarover het OR-lid als zodanig kan beschikken. De wetsgeschiedenis van artikel 17 WOR maakt helder dat tussen de OR en de werkgever geen gezagsrelatie bestaat. De werkgever kan zijn gezagsbevoegdheid dus niet aanwenden om het e-mailgebruik van OR-leden in functie te controleren. Dit betekent dat op e-mail van, aan en tussen OR-leden in functie de algemene wettelijke regels omtrent vertrouwelijke communicatie van toepassing zijn. In het LOGA d.d. 23 december 2004 is geconcludeerd dat GO-leden (GO: Georganiseerd Overleg) zich in een soortgelijke positie bevinden. Om die reden is besloten de gedragslijn voor OR-leden ook te hanteren voor GO-leden.
Daarmee is dit soort e-mail geprivilegieerd en mag de werkgever er in beginsel geen kennis van nemen. Het betreft hier echter geen absoluut verbod. Er kan van worden afgeweken in bepaalde situaties van plichtsverzuim, zoals geregeld in artikel 16:1:1 lid 2 van de Uitwerkingsovereenkomst (UWO), waarbij men bijvoorbeeld kan denken aan het lekken van geheime c.q. vertrouwelijke stukken.

Daarnaast ziet deze bepaling ook toe op het gebruik van internet. Het Cbp heeft de VNG in een brief d.d. 22 september 2004 laten weten dat artikel 6, zesde lid niet alleen geldt voor het gebruik van e-mailfaciliteiten, maar ook voor internetgebruik. Dit standpunt van het Cbp heeft de VNG in haar privacyreglement verwerkt, maar is nog niet opgenomen in de ‘Raamregeling voor het gebruik van e-mail en internet’ van het Cbp.

<u>Artikel 7</u> Bewaring en verwijdering

Artikel 7, eerste lid

1. *Persoonsgegevens, gerelateerd aan de elektronische communicatiemiddelen, worden maximaal zes maanden bewaard. Gegevens die ouder zijn dan zes maanden worden automatisch verwijderd, tenzij er bijzondere redenen zijn, zoals een zwaarwegend vermoeden van onrechtmatig gebruik dan wel misbruik van de elektronische communicatiemiddelen, om de gegevens langer te bewaren. Dat moet dan expliciet kunnen worden gemaakt en worden gemeld aan het Cbp.*

Het is in het algemeen niet nodig om de persoonsgegevens lang te bewaren. De standaardtermijn is daarom zes maanden. In het geval van een zwaarwegend vermoeden van onrechtmatig gebruik dan wel misbruik van elektronische communicatiemiddelen, worden de gegevens uit die zes maanden bewaard, zolang dit in het kader van nader onderzoek en eventueel te treffen maatregelen jegens een medewerker noodzakelijk is. Zodra een nader onderzoek is afgerond en dit niet leidt tot maatregelen jegens een medewerker worden de gegevens verwijderd.

In relatie tot de termijn gedurende welke persoonsgegevens mogen worden bewaard, kan het volgende worden opgemerkt. De termijn gedurende welke de in archiefbescheiden opgenomen persoonsgegevens mogen worden bewaard, is in beginsel onbepaald. Deze onbepaalde termijn houdt direct verband met het doeleinde waarvoor de gegevens worden bewaard: behoud van (een deel van) het Nederlandse culturele erfgoed.

Artikel 7, tweede lid
Bepaalde gegevens kunnen soms om technische redenen niet worden verwijderd. Van het e-mailsysteem worden bijvoorbeeld back-ups gemaakt die in geval van nood teruggezet kunnen worden. Deze back-ups kunnen niet zonder meer gewist worden. Het is ook niet mogelijk om binnen een dergelijke back-up een individueel e-mailbericht te verwijderen. De bedoelde gegevens mogen in deze gevallen niet meer worden verstrekt (verwerkt).

Artikel 8 Rechten van de medewerker
In artikel 8 worden de rechten van de medewerkers bij het verwerken van persoonsgegevens behandeld. Transparantie is een belangrijk beginsel voor privacybescherming. De informatieplicht is gebaseerd op de artikelen 33 en 34 WBP.

Artikel 9 Sancties
In de herziene versie van het VNG model is het eerste lid opnieuw geformuleerd waarbij ontslag als disciplinaire straf expliciet wordt genoemd.

1. *Overtreding van dit privacyreglement kan voor werknemers in dienst van de gemeente resulteren in disciplinaire maatregelen of ontslag als disciplinaire straf als bedoeld in de arbeidsvoorwaardenregeling van de gemeente Groningen (ARG).*

De toevoeging is voor alle zekerheid opgenomen, zie ook uitspraak d.d. 8 juni 2004 van de voorzieningenrechter van de Centrale Raad van Beroep over internetmisbruik door een ambtenaar van een gemeente (Zie LJN-nummer: AP9387). De rechtbank oordeelde in eerdere instantie dat het strafontslag niet evenredig was aan de aard en ernst van het plichtsverzuim. Bovendien was de ambtenaar van tevoren niet gewaarschuwd dat dergelijk gedrag tot de zwaarst mogelijke disciplinaire maatregel zou kunnen leiden. De gemeente tekende hoger beroep aan en diende tevens een schorsingsverzoek in bij de voorzieningenrechter van de Centrale Raad van Beroep. Deze oordeelde: ‘met de gemeente is de voorzieningenrechter van oordeel dat het feit dat in het e-mail- en internetprotocol van de gemeente niet is opgenomen dat gedragingen als de onderhavige voor de betrokken ambtenaar tot de zwaarst mogelijke disciplinaire maatregel kunnen leiden, niet met zich brengt dat gemeente niet bevoegd is een dergelijke straf op te leggen. Gemeente is immers op grond van het ARG bevoegd een ambtenaar disciplinair te straffen wanneer deze iets doet wat een goed ambtenaar behoort na te laten.’ De uitspraak van het hoger beroep was echter ten tijde van de actualisering van het privacyreglement nog niet bekend.

Tegen het opleggen van disciplinaire maatregelen/straffen kan op basis van de Algemene wet bestuursrecht (Awb) bezwaar en beroep worden aangetekend.

Bij het tweede lid, onder sub b zijn voor de gemeente Groningen aanvullende sancties opgenomen. Te weten: het ontbinden van de overeenkomst en het geven van een waarschuwing.

Artikel 10 Onvoorziene omstandigheden
Bij onvoorziene omstandigheden beslist het college. Dit artikel behoeft geen nadere uitleg.

Artikel 11 Openbaarmaking, inwerkingtreding en evaluatie
Het privacyreglement moet helder naar de medewerkers worden gecommuniceerd. De medewerkers moeten weten wat verboden is en wat is toegestaan, dat controle mogelijk is, op welke manier die controle geschiedt en wat de consequenties zijn bij overtreding van het privacyreglement. Het reglement kan bijvoorbeeld naast verstrekking op papier, tevens op het beeldscherm van medewerkers worden gepresenteerd tijdens het opstarten van het systeem of van het programma. Op die manier is verzekerd dat de medewerkers zich bewust zijn van het privacyreglement.

In het derde lid is opgenomen:

3. *Dit privacyreglement wordt tweejaarlijks geëvalueerd door de verantwoordelijke en de ondernemingsraden van de Bestuursdienst en Griffie, Dienst Informatie en Administratie, Dienst Sociale Werkvoorziening Stadspark, Hulpverleningsdienst, Milieudienst, Onderwijs Cultuur Sport Welzijn, Ruimtelijke Ordening en Economische Zaken, Sociale Zaken en Werk.*

Het beheer van het privacyreglement is belegd bij de afdeling BJZ van de Bestuursdienst. Zij dragen zorg voor bewaring en de, in het reglement vastgelegde, tweejaarlijkse evaluatie, dan wel eerder indien omstandigheden dit vereisen.

Artikel 12 Slotbepaling

Elektronische controle van computergebruik raakt het terrein van de bescherming van de persoonlijke levenssfeer van de medewerker. Op het controleren van het gebruik van e-mail en internet op de werkplek is daarom de Wet bescherming persoonsgegevens (WBP) van toepassing die op 1 september 2001 in werking is getreden.