Gemeente Raalte

GEMEENTEBLAD

Officiële uitgave van de gemeente Raalte

Nr. 158799

31 juli

2018

Gemeente Raalte Privacyreglement e-mail- en internetgebruik griffie

De raad van de Gemeente Raalte;
Gelezen het voorstel van de agendacommissie met zaaknummer 11290-2018
Gelet op de Gemeentewet;

Besluit:
Vast te stellen de regeling Privacyreglement e-mail- en internetgebruik griffie Raalte

Hoofdstuk 1 Definities, reikwijdte en doeleinden

Artikel 1 Definities

a. Wbp: Wet bescherming persoonsgegevens.
b. Gemeente: De gemeente Raalte
c. Cbp: College bescherming persoonsgegevens.
d. Medewerker: Degene die aan te merken is als:
    a. persoon met een aanstelling bij of een arbeidsovereenkomst met de gemeente Raalte.
    b. persoon die (betaalde of niet-betaalde) werkzaamheden voor de gemeente verricht, anders dan in ambtelijk dienstverband.

e. E-mailfaciliteiten: De door of namens de gemeente aan medewerkers ter beschikking gestelde e-mailfaciliteiten.
f. Internetfaciliteiten: De door of namens de gemeente aan medewerkers ter beschikking gestelde internetfaciliteiten.
g. Elektronische communicatiemiddelen: E-mail- en/of internetfaciliteiten.
h. Persoonsgegeven: Elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon in de zin van de Wbp.
i. Systeembeheerder: De door het college van burgemeester en wethouders in het kader van deze regeling als zodanig aangewezen personen.
j. Verwerken van persoonsgegevens: Elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens.
k. Verantwoordelijke: Het college, zijnde het bestuursorgaan dat het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.
l. Onrechtmatig gebruik dan wel misbruik van de elektronische communicatiemiddelen: Een doen of nalaten in strijd met dit privacyreglement of andere wet- en regelgeving of een inbreuk op een recht.

Artikel 2 Reikwijdte

1. Dit privacyreglement is van toepassing op het verwerken van persoonsgegevens inzake het gebruik van elektronische communicatiemiddelen. Dit privacyreglement geeft de wijze aan waarop in de gemeente wordt omgegaan met elektronische communicatiemiddelen en omvat regels ten aanzien van verantwoord gebruik hiervan en regels over de wijze waarop controle hiervan plaatsvindt.
2. Dit privacyreglement geldt voor werknemers in dienst van de gemeente en personen die (betaalde of niet-betaalde) werkzaamheden voor de gemeente verrichten, anders dan in ambtelijk dienstverband.
3. Dit privacyreglement geldt voor de dagelijks bestuurders van de gemeente. Daar waar de secretaris wordt genoemd als bevoegd gezag, wordt in het geval van overtredingen door dagelijks bestuurders de burgemeester in de plaats gelezen. Daar waar beklag de burgemeester betreft, zijn de wethouders in gezamenlijkheid het aanspreekpunt dat kan beslissen over nader onderzoek en het aanspreken van de burgemeester.

Artikel 3 Doeleinden

De verwerking van persoonsgegevens inzake het gebruik van de elektronische communicatiemiddelen heeft de volgende doeleinden:
a. het verkrijgen van inzicht in de mate van gebruik van de elektronische communicatiemiddelen;
b. controle ter toetsing van het verantwoorde gebruik van elektronische communicatiemiddelen;
c. het beveiligen van het systeem en het netwerk.

Hoofdstuk 2 Verantwoordelijkheden en beheer

Artikel 4 Verantwoordelijkheden en beheer

1. Door de verantwoordelijke worden de nodige maatregelen getroffen opdat persoonsgegevens, gelet op de doeleinden waarvoor zij worden verwerkt, juist en nauwkeurig zijn.
2. Door de verantwoordelijke worden passende technische en organisatorische maatregelen ten uitvoer gelegd om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking.
3. Door de verantwoordelijke worden één of meerdere systeembeheerders aangewezen die belast zijn met het beheer van het (de) bestand(en). Deze systeembeheerders zijn, op grond van artikel 125a, derde lid, Ambtenarenwet, verplicht tot geheimhouding van de persoonsgegevens waarvan zij kennisnemen, behoudens voorzover enig wettelijk voorschrift hen tot mededeling verplicht of uit hun taak de noodzaak tot mededeling voortvloeit.

Hoofdstuk 3 Gebruik elektronische communicatiemiddelen

Artikel 5 Gebruik elektronische communicatiemiddelen

1. Medewerkers gebruiken de elektronische communicatiemiddelen primair voor het uitvoeren van de aan hen door de gemeente opgedragen taken.
2. Incidenteel privégebruik van de elektronische communicatiemiddelen door medewerkers is toegestaan mits dit gebruik in overeenstemming is met dit privacyreglement en dit gebruik in geen geval storend is voor dan wel ten koste gaat van het uitvoeren van de aan hen door de gemeente opgedragen taken.
3. Het is medewerkers 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. Evenmin is het medewerkers 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 medewerker redelijkerwijs moet aannemen dat deze te omvangrijk zijn.
4. Het is medewerkers 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 oneervol worden beschouwd;
   - mee te doen in chat-sessies;
   - on line te gokken;
   - illegale software te downloaden
   - zonder voorafgaand overleg met de systeembeheerder(s) bestanden te downloaden waarvan medewerker redelijkerwijs moet aannemen dat deze te omvangrijk zijn.
     Het verbod geldt niet indien een dergelijk gebruik van de internetfaciliteiten plaatsvindt in het kader van en noodzakelijk is voor het uitvoeren van de werkzaamheden.

5. Zonder voorafgaande toestemming van de systeembeheerder(s) is het medewerkers niet toegestaan met behulp van de e-mailfaciliteiten een elektronisch bericht aan alle of vrijwel alle medewerkers van de gemeente tegelijkertijd te versturen.
6. Indien medewerkers met gebruik van de internetfaciliteiten handelingen verrichten die als e-mailtoepassingen zijn te kwalificeren, dan zijn de bepalingen van artikel 5, derde en vijfde lid, van overeenkomstige toepassing.
7. Medewerkers zullen bij het gebruik van de elektronische communicatiemiddelen de nodige zorgvuldigheid betrachten en de integriteit en goede naam van de gemeente waarborgen.

Hoofdstuk 4 Controle, bewaring en verwijdering persoonsgegevens

Artikel 6 Controle

1. Controle door verantwoordelijke op het gebruik van de elektronische communicatiemiddelen vindt slechts plaats in het kader van de in artikel 3 genoemde doeleinden. Deze doeleinden stellen beperkingen aan de omvang en wijze van controle.
   a. Controle ter verkrijging van inzicht in de mate van gebruik van de elektronische communicatiemiddelen wordt beperkt tot de verkeersgegevens (tijd, hoeveelheid, omvang).
   b. Controle ter toetsing van het verantwoorde gebruik van elektronische communicatiemiddelen, 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.
   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.

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.
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.
4. Onrechtmatig gebruik dan wel misbruik van de elektronische communicatiemiddelen wordt zo veel mogelijk softwarematig onmogelijk gemaakt.
5. Indien geconstateerd wordt dat een medewerker dit privacyreglement overtreedt, dan wordt de betrokken medewerker zo spoedig mogelijk hierop aangesproken door Raalte.
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.

Artikel 7 Bewaring en verwijdering

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, bijvoorbeeld 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.
2. Indien de systeembeheerder om technische redenen persoonsgegevens, gerelateerd aan de elektronische communicatiemiddelen, niet kan verwijderen, wordt onder verwijderen verstaan het niet meer verstrekken van deze gegevens voor de in artikel 3 geformuleerde doeleinden.

Hoofdstuk 5 Rechten van medewerker: verbeteren, aanvullen, verwijderen of afschermen persoonsgegevens

Artikel 8 Rechten van de medewerker

1. Aan de medewerker die daarom aan verantwoordelijke verzoekt wordt een overzicht verschaft van de hem betreffende persoonsgegevens die worden verwerkt.
2. De medewerker kan de verantwoordelijke verzoeken zijn persoonsgegevens te verbeteren, aan te vullen, te verwijderen of af te schermen 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. Het verzoek bevat de aan te brengen wijzigingen.
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 6 Sancties, onvoorziene omstandigheden, openbaarmaking, inwerkingtreding, evaluatie en slotbepaling

Artikel 9 Sancties

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.
2. Overtreding van dit privacyreglement 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. het geven van een waarschuwing en/of het ontbinden van de overeenkomst.

Artikel 10 Onvoorziene omstandigheden

In gevallen waarin dit privacyreglement niet voorziet of bij twijfel omtrent de toepassing van dit privacyreglement, beslist de gemeenteraad.

Artikel 11 Openbaarmaking, inwerkingtreding en evaluatie

Dit privacyreglement wordt verstrekt of ter beschikking gesteld aan alle medewerkers die, direct of indirect, de beschikking krijgen over elektronische communicatiemiddelen.

Deze regeling treedt in werking op de dag volgend op die waarop de bekendmaking heeft plaats gevonden.

Deze regeling kan worden aangehaald als de regeling privacyreglement e-mail-en internetgebruik griffie Raalte.
Aldus besloten door de raad in zijn openbare vergadering van 12 juli 2018.

Griffier,
Jan Bouke Zijlstra
Voorzitter,
Martijn Dadema

Toelichting: Algemene en artikelsgewijze toelichting

Algemeen
Vooraf
Binnen gemeenten wordt veel gebruikgemaakt van e-mail en internet. Om het gebruik van e-mail en internet in goede banen te leiden, kunnen gedragscodes en gebruiksregels worden opgesteld die door middel van controle worden gehandhaafd. Uit onderzoek naar rechtspraak over e-mail- of internetmisbruik blijkt dat de aanwezigheid van een gedragscode zeer relevant is. Het is voor gemeenten dan ook zaak daarover een duidelijk beleid te voeren. Elektronische controle van computergebruik raakt echter 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.
Dit reglement biedt een juridisch kader in geval van excessen. De gemeente streeft naar een cultuur waarin de organisatie en de medewerkers gezamenlijk zorg dragen en verantwoordelijkheid nemen voor een vanzelfsprekend verantwoord gebruik van e-communicatiemiddelen.
Het controleren van e-mail- en internetgebruik is een zogenaamd personeelvolgsysteem. Voor de invoering van een personeelvolgsysteem en een privacyreglement is op grond van artikel 27, eerste lid, onder k en l, van de Wet op de ondernemingsraden, de instemming van de ondernemingsraad (OR) vereist. Dit geldt ook voor een eventuele latere wijziging of bij intrekking van het reglement. Na instemming van de OR kan het reglement op de voor gemeenten gebruikelijke wijze worden vastgesteld en ingevoerd.
Een verantwoordelijke is verplicht om de verwerking van persoonsgegevens te melden bij het College bescherming persoonsgegevens (Cbp) voordat hij begint met de verwerking. In het zogenaamde Vrijstellingsbesluit staan eisen geformuleerd waaraan de verwerkingen moeten voldoen, wil de vrijstelling van de meldingsverplichting daadwerkelijk gelden. Op basis van het Vrijstellingsbesluit valt controle op het gebruik van e-mail en internet onder de vrijstelling mits voldaan wordt aan de vereisten van het Vrijstellingsbesluit. Deze vereisten houden in dat geen andere persoonsgegevens worden verwerkt dan: a) gegevens ten behoeve van identificatie van en communicatie (username en toegangscode) met de gebruikers binnen het netwerk; b) gegevens met betrekking tot bevoegdheden van de gebruikers en de netwerkbeheerders met het oog op de aangeboden faciliteiten en diensten van het netwerk; c) gegevens met betrekking tot de verrichtingen van de gebruikers en netwerkbeheerders en d) gegevens met betrekking tot elektronische berichten van of voor de gebruikers. Daarnaast geldt dat de persoonsgegevens slechts worden verstrekt aan degenen die belast zijn met de interne controle en beveiliging (de doeleinden van de verwerking), met dien verstande dat verstrekking aan derden slechts geschiedt met het oog op het behandelen van geschillen. Bovendien dienen de persoonsgegevens uiterlijk zes maanden nadat ze zijn verkregen te worden verwijderd dan wel twee jaar nadat het dienstverband of de werkzaamheden van betrokkenen ten behoeve van de verantwoordelijke zijn beëindigd. Ten slotte geldt dat de OR aan de controle instemming heeft verleend.
Het in 2001 opgestelde VNG voorbeeld-privacyreglement e-mail- en internetgebruik (hierna ook: privacyreglement) heeft in 2002 en 2003 een aantal kleine wijzigingen ondergaan. De herziening die nu in 2004 heeft plaatsgevonden is fundamenteler van aard. Het privacyreglement is qua opzet vereenvoudigd conform de Raamregeling van het Cbp. Tevens is het aangepast aan de actuele ontwikkelingen (bijvoorbeeld het gebruik van content filtering) en relevante jurisprudentie. Het reglement is daarom (net als in 2001) naar het Cbp gestuurd en vervolgens aangepast aan de opmerkingen en aanbevelingen van het Cbp. Het Cbp heeft in een schriftelijk schrijven aangegeven dat naar zijn oordeel het privacyreglement in overeenstemming is met het rapport Goed werken in netwerken van het Cbp en de daarin opgenomen vuistregels voor controle op het gebruik van e-mail en internet van werknemers en daarom niet strijdig is met de huidige privacywetgeving. Het reglement is tevens behandeld in de commissies Juridische zaken en Informatiebeleid van de VNG. Beide commissies hebben ingestemd met verzending van het reglement aan de gemeenten. Ten slotte is het reglement besproken in en akkoord bevonden door het Landelijk Overleg Gemeentelijke Arbeidsvoorwaarden (LOGA).
Omdat het college geen zeggenschap heeft over de medewerkers van de griffie (en het wel wenselijk is om ook deze medewerkers onder de regeling te laten vallen), moet het Reglement ook door de raad worden vastgesteld.
Artikel 1
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.

In het vierde lid is 'Betrokkene' gewijzigd in 'Medewerker'. Deze wijziging is in het gehele reglement doorgevoerd. De definitie van 'Bestand' in het negende lid is verwijderd omdat het woord 'Bestand' – zoals gedefinieerd in deze zin – niet meer in het privacyreglement voorkomt.
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.

Artikel 2

Het privacyreglement is van toepassing op het verwerken van persoonsgegevens inzake het gebruik van e-mail en/of internetfaciliteiten.
Aan het bepaalde in het eerste lid van dit artikel is toegevoegd (nieuw):
Dit privacyreglement geeft de wijze aan waarop in de gemeente wordt omgegaan met elektronische communicatiemiddelen en omvat regels ten aanzien van verantwoord gebruik hiervan en regels over de wijze waarop controle hiervan plaatsvindt.
Het privacyreglement geldt voor alle medewerkers van de gemeente: ambtenaren en personen die (betaald of niet-betaald) werkzaamheden voor de gemeente verrichten, anders dan in ambtelijk dienstverband. In het tweede lid is 'medewerkers' gewijzigd in 'werknemers' (in verband met de wijziging van de definitie in artikel 1, vierde lid).
Bestuurders
Het privacyreglement is ook van toepassing verklaard op het college van burgemeester en wethouders.
Telewerken
Indien de werknemer vanuit zijn eigen huis inlogt op het computersysteem van het werk (telewerken), dan vormt de controle door de werkgever op het gebruik door de werknemer van de elektronische communicatiemiddelen een extra probleem. Voor zover de werknemer uitsluitend ten behoeve van het werk inlogt, zijn de regels in dit privacyreglement van overeenkomstige toepassing. De computer van de werknemer thuis maakt dan immers logisch gezien deel uit van het computernetwerk van de werkgever en de werknemer bevindt zich in een situatie waarin ook de gezagsbevoegdheid van de werkgever geldt. Dit geldt evenzo voor de situaties waar op een andere locatie dan vanuit het eigen huis werkzaamheden voor de gemeente worden uitgevoerd.
Dit ligt anders als de werknemer het bedrijfsaccount voor privé-doeleinden kan en mag gebruiken (om privé-e-mail te versturen of in zijn eigen tijd internetsites te bezoeken). Voor het vastleggen van gegevens van hetgeen de werknemer privé doet, is geen grond. Indien ook zijn gezinsleden van de faciliteiten gebruik mogen maken, geldt dit helemaal. De werkgever heeft met hen immers geen arbeidsrelatie waarin hij zijn gezag kan uitoefenen. Zijn positie is in deze situatie vergelijkbaar met een Internet Service Provider. De werkgever dient hiermee rekening te houden bij het opzetten en de uitvoering van het telewerkbeleid.

Artikel 3

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 drie doeleinden geformuleerd.
Onderdeel c is toegevoegd (nieuw)
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

Lid 1
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.
Lid 2
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.
Lid 3
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

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

Dit artikel is voor een groot deel nieuw. De in het oude privacyreglement opgenomen specificatie van vastgelegde persoonsgegevens en het onderscheid tussen 'vastleggen' en 'verstrekken' is komen te vervallen omdat dit niet noodzakelijk is. Dit is overlegd met het Cbp die in haar eigen raamregeling ook niet zo'n specificatie c.q. onderscheid hanteert (Cbp-raamregeling werkt met het begrip 'controle').
Binnen de organisatie worden overzichten verstrekt in verband met de doeleinden als genoemd in artikel 3:
§ doeleinde onder a en c: vastgelegde gegevens worden (na bewerking) verstrekt aan het voor automatisering verantwoordelijke hoofd voor het verkrijgen van inzicht in de mate van gebruik van de elektronische communicatiemiddelen;
§ doeleinde b: de verantwoordelijke of degene(n) die op verzoek van de verantwoordelijke is (zijn) belast met of leiding geeft (geven) aan onderzoek naar onrechtmatig gebruik of misbruik van de elektronische communicatiemiddelen.
Lid 1, 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.
Lid 1, onder sub b
De eerste zin van deze bepaling was opgenomen in artikel 3, tweede lid (oud). Aan het bepaalde in het eerste lid, onder sub b is een tweede zin toegevoegd (nieuw).
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. Indien de gemeente gebruik gaat maken van content filtering, dan dient dit expliciet in het privacyreglement of in de toelichting te worden opgenomen.
Lid 1, onder sub c
Sub c is nieuw
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 privémail.
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.
Lid 2
Het tweede lid is nieuw
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.
Lid 3
Het derde lid is nieuw
Lid 4
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.
Lid 5
Het vijfde lid is nieuw
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. In de praktijk wordt de medewerker door diens leidinggevende aangesproken en in de gelegenheid gesteld hierop te reageren.
Lid 6
Het zesde lid is nieuw
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.
Concrete verdenking
In geval van een concrete verdenking kan er gerichte controle plaatsvinden.
Controle op inhoud kan alleen bij zwaarwegende redenen en daartoe moet speciaal schriftelijk opdracht worden gegeven door de gemeentesecretaris. Per geval moet de gemeentesecretaris afwegen of overgegaan wordt tot gerichte controle (maatwerk). Daarbij wordt de exacte periode omschreven, die zo beperkt mogelijk wordt gehouden.
In het onderzoek wordt zoveel mogelijk gewerkt met het "vier ogen beginsel", zodat de onderzoeker een buddy heeft waarmee hij of zij de gegevens kan verwerken en interpreteren. De buddy kan ook externe hulp zijn.
Wie van de onderzoeksresultaten op de hoogte kunnen komen, zijn de gemeentesecretaris, de leidinggevenden die in lijn boven de persoon staat die het onderzoek betreft, de uitvoerders van het onderzoek (inclusief evt. externe deskundigen), de HRM-adviseurs die in die casus adviseren en alle anderen die op formele gronden van de feiten op de hoogte gebracht dienen te worden. In die laatste categorie zitten in elk geval het college, dat als dagelijks bestuur verantwoordelijk is voor de organisatie, maar ook de politie waarbij in geval van ambtsmisdrijven verplicht aangifte moet worden gedaan.
Omdat controle en onderzoek ingrijpend kunnen zijn voor de privacy van de onderzochte personen, wordt van specifiek opgedragen onderzoek getalsmatig verslag gedaan aan de OR.
Artikel 7
Lid 1
Het eerste lid is geherformuleerd.
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. De gemeentesecretaris dient opdracht te geven voor het verlengen van de duur van de bewaring van (onderzoeks)gegevens.
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.
Lid 2

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

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.

In het eerste lid (nieuw) is de tweede zin 'Indien een gewichtig belang van de verzoeker dit eist, voldoet de verantwoordelijke aan dit verzoek in een andere dan schriftelijke vorm, die aan dat belang is aangepast' uit het eerste lid (oud) verwijderd. Hiertoe is besloten vanwege de gewenste vereenvoudiging van het privacyreglement. Een medewerker kan zich hier echter nog altijd op beroepen omdat deze bepaling ook is opgenomen in artikel 37, eerste lid WBP.

Gelet op de gewenste vereenvoudiging van het privacyreglement is ook het eerste deel van de eerste zin in het tweede lid 'Degene aan wie overeenkomstig het eerste lid kennis is gegeven van de hem betreffende persoonsgegevens' uit het tweede lid (oud) verwijderd.

Artikel 9

Het eerste lid (nieuw) is opnieuw geformuleerd waarbij ontslag als disciplinaire straf expliciet wordt genoemd. Het eerste lid is geherformuleerd.

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.

In het eerste lid is 'medewerkers' bovendien gewijzigd in 'werknemers' (in verband met de wijziging van de definitie in artikel 1, derde lid).

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

Het tweede lid, onder sub b is nader worden ingevuld met het ontbinden van de overeenkomst en het geven van een waarschuwing.

Artikel 10

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

Artikel 11

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. Het derde lid is nieuw.

Artikel 12

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.