Gemeente Almere

GEMEENTEBLAD

Officiële uitgave van de gemeente Almere

Nr. 227929

26 oktober

2018

PRIVACYREGLEMENT E-MAIL- EN INTERNETGEBRUIK GEMEENTE ALMERE 2018

Burgemeester en wethouders van de gemeente Almere;

gelet op:
- het feit dat de gemeente Almere aan degenen die bij haar organisatie werkzaam zijn en politieke ambtsdragers e-mail- en internetfaciliteiten ter beschikking stelt om met behulp daarvan hun (politieke) functie uit te oefenen;
- de wenselijkheid een (geactualiseerd) Privacyreglement vast te stellen, waarin naast regels voor e-mail- en internetgebruik eveneens regels zijn opgenomen voor het monitoren van dit gebruik;
- het bepaalde in de Algemene Verordening Gegevensbescherming;
- het bepaalde in de Archiefwet 1995 en de daaruit voortvloeiende regelgeving;
- de op 26 juni 2017 verleende instemming van de Ondernemingsraad met het Privacyreglement;

besluiten:

het volgende **Privacyreglement e-mail- en internetgebruik 2018** vast te stellen:

HOOFDSTUK 1 DEFINITIES, REIKWIJDTE EN DOELEINDEN

Artikel 1 Definities

In dit Privacyreglement wordt verstaan onder:
1. AVG: Algemene Verordening Gegevensbescherming;
2. Gemeente: de gemeente Almere;
3. AP: Autoriteit Persoonsgegevens;
4. Politieke ambtsdrager: een lid van het college;
5. Medewerker: degene die aan te merken is als:
   a. werknemer in dienst van de gemeente;
   b. persoon die (betaalde of niet-betaalde) werkzaamheden voor de gemeente verricht, anders dan in ambtelijk dienstverband;
6. E-mail faciliteiten: de door of namens de gemeente aan medewerkers en politieke ambtsdragers ter beschikking gestelde e-mail faciliteiten;
7. Internet faciliteiten: de door of namens de gemeente aan medewerkers en politieke ambtsdragers ter beschikking gestelde internet faciliteiten;
8. Elektronische communicatiemiddelen: e-mail- en/of internetfaciliteiten;
9. Persoonsgegeven: elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon in de zin van de AVG;
10. 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;
11. Verwerkingsverantwoordelijke: het college van burgemeester en wethouders, zijnde het bestuursorgaan dat het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt;
12. 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 medewerkers van de gemeente en politieke ambtsdragers.

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. het voorkomen van onrechtmatig gebruik dan wel misbruik van de elektronische communicatiemiddelen;
c. het beveiligen van het systeem en het netwerk;
d. bewijs en archivering.
e. continuïteit van de bedrijfsvoering en de dienstverlening.

HOOFDSTUK 2 VERANTWOORDELIJKHEDEN EN BEHEER

Artikel 4 Verantwoordelijkheden en beheer

1. Door de verwerkingsverantwoordelijke worden de nodige maatregelen getroffen opdat persoonsgegevens, gelet op de doeleinden waarvoor zij worden verwerkt, juist en nauwkeurig zijn.
2. Door de verwerkingsverantwoordelijke 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 verwerkingsverantwoordelijke worden één of meerdere beheerders aangewezen die belast zijn met het beheer van het (de) bestand(en). Deze beheerders 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.
4. Medewerkers zijn ingeval van uitdiensttreding c.q. ontslag zelf verantwoordelijk voor het verwijderen van privé-mail en privé bestanden. Politieke ambtsdragers zijn in geval van beëindiging van hun functie zelf verantwoordelijk voor het verwijderen van privé-mail en privé bestanden.
5. Langdurige ziekte, ontslag, uitdiensttreding en noodsituaties kunnen met het oog op het bedrijfsbelang reden zijn om toegang tot de mailbox of bestanden van een medewerker te krijgen, waarbij rekening wordt gehouden met de geldende normen met betrekking tot kennisneming van privé-mail / bestanden.
6. Na uitdiensttreding c.q. ontslag kan een analyse van de mailbox of bestanden van de ex-medewerker plaatsvinden, met inachtneming van de normen zoals bedoeld in het vijfde lid.

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. Politieke ambtsdragers gebruiken de elektronische communicatiemiddelen primair voor de uitvoering van hun politieke functie in de gemeente.
2. Incidenteel privé-gebruik van de elektronische communicatiemiddelen door medewerkers en politieke ambtsdragers 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 respectievelijk het uitvoeren van hun (politieke) functie.
3. Het is medewerkers en politieke ambtsdragers niet toegestaan met behulp van e-mail faciliteiten 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 en politieke ambtsdragers toegestaan met behulp van de e-mail faciliteiten illegale software te verzenden of op te vragen dan wel bestanden zonder voorafgaand overleg met de Technisch Architect te verzenden of op te vragen waarvan men redelijkerwijs moet aannemen dat deze te omvangrijk zijn.
4. Het is medewerkers en politieke ambtsdragers niet toegestaan met behulp van de internet faciliteiten 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 dan wel zonder voorafgaand overleg met de Technisch Architect bestanden te downloaden waarvan men redelijkerwijs moet aannemen dat deze te omvangrijk zijn. Medewerkers die op basis van hun functie het recht hebben om een onderzoek en/of controle uit te voeren, zijn uitgezonderd van het verbod om bovengenoemde internetsites te bezoeken, mits zij

hiervoor, uit hoofde van hun onderzoeks- en controletaken, ook specifiek toestemming van de leidinggevende, hebben.
5. Zonder voorafgaande toestemming van de afdeling Communicatie is het medewerkers en de politieke ambtsdrager niet toegestaan met behulp van e-mail faciliteiten een elektronisch bericht aan alle of vrijwel alle medewerkers van de gemeente tegelijkertijd te versturen.
6. Indien medewerkers en politieke ambtsdragers met gebruik van internet faciliteiten 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 en politieke ambtsdragers 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 verwerkingsverantwoordelijke 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 en dergelijke).
   b. Controle ter voorkoming van onrechtmatig gebruik dan wel misbruik van de elektronische communicatiemiddelen 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.
   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.
   d. Controle zal moeten voldoen aan de juiste bewijsvoering

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. Controle op de inhoud vindt slechts plaats na goedkeuring door de gemeentesecretaris.
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 de leidinggevende.
6. Het gebruik van de elektronische communicatiemiddelen door bijvoorbeeld OR-leden, GO-leden, mediators, bedrijfsartsen, andere medewerkers met een vertrouwensfunctie en politieke ambtsdragers zijn in beginsel uitgesloten van controle. Dit geldt niet voor de controle op de veiligheid van het elektronische verkeer.
7. De burgemeester kan, indien er een redelijk vermoeden bestaat van onrechtmatig gebruik dan wel misbruik van de elektronische communicatiemiddelen, opdracht geven bij een bepaalde politieke ambtsdrager voor een aangegeven periode een omschreven controle op zijn gebruik van de elektronische communicatiemiddelen toe te passen. Over de controle wordt rapport aan de burgemeester uitgebracht.

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.
2. Indien de informatiebeheerder 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 EN POLITIEKE AMBTSDRAGER: VERBETEREN, AANVULLEN, VERWIJDEREN OF AFSCHERMEN PERSOONSGEGEVENS

Artikel 8 Rechten van de medewerker en politieke ambtsdrager

1. Aan de medewerker en de politieke ambtsdrager die daarom aan verwerkingsverantwoordelijke verzoekt, wordt een overzicht verschaft van de hem betreffende persoonsgegevens die worden verwerkt.
2. De medewerker en de politieke ambtsdrager kan de verwerkingsverantwoordelijke 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 verwerkingsverantwoordelijke 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 verwerkingsverantwoordelijke 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 ontzeggen van de toegang en/of verblijf van de kantoren, werkplaatsen of andere arbeidsterreinen;
   c. het ontbinden van de overeenkomst.
   d. verbod om nog langer werkzaamheden voor de gemeente te verrichten.
3. Overtreding van dit Privacyreglement kan voor politieke ambtsdragers resulteren in sanctiemogelijkheden, conform de Gedragscode integriteit burgemeester en wethouders gemeente Almere 2016.
4. Bij strafbare feiten kan door of vanwege de gemeente aangifte worden gedaan.

Artikel 10 Onvoorziene omstandigheden

In gevallen waarin dit Privacyreglement niet voorziet of bij twijfel omtrent de toepassing van dit Privacyreglement, beslissen burgemeester en wethouders.

Artikel 11 Openbaarmaking, inwerkingtreding en evaluatie

1. Dit Privacyreglement wordt openbaar gemaakt ten behoeve van alle medewerkers en politieke ambtsdragers die, direct of indirect, de beschikking krijgen over elektronische communicatiemiddelen.
2. Dit Privacyreglement treedt in werking op de dag na bekendmaking, onder gelijktijdige intrekking van het Privacyreglement e-mail- en internetgebruik, vastgesteld door burgemeester en wethouders op 15 juni 2004 en in werking getreden met ingang van 1 juli 2004.
3. Dit Privacyreglement wordt vierjaarlijks geëvalueerd door de verwerkingsverantwoordelijke en de Ondernemingsraad.

Artikel 12 Slotbepaling

Onverminderd het bepaalde in dit Privacyreglement, zal op het verwerken van persoonsgegevens de AVG van toepassing zijn.

Aldus vastgesteld in de vergadering van het college van burgemeester en wethouders van 16 oktober 2018,
burgemeester en wethouders van Almere,

de secretaris, de burgemeester,
R. Wielinga F.M. Weerwind

Toelichting

Behorende bij het Privacyreglement e-mail- en internetgebruik gemeente Almere 2018

Algemeen
Binnen de gemeente Almere 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 de gemeente dan ook zaak daarover een duidelijk beleid te voeren. Elektronische controle van computergebruik raakt echter het terrein van de bescherming van de persoonlijke levenssfeer. Op het controleren van het gebruik van e-mail en internet op de werkplek is daarom de AVG van toepassing.

Het controleren van e-mail- en internetgebruik is een zogenaamd personeelsvolgsysteem. Voor de invoering van een personeelsvolgsysteem 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 de gemeente gebruikelijke wijze worden vastgesteld en ingevoerd.

Het Privacyreglement is qua opzet vereenvoudigd conform de Raamregeling van het AP. Tevens is het aangepast aan de relevante ontwikkelingen en relevante jurisprudentie.

Artikelsgewijze toelichting

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 AVG

De AVG is van toepassing als er sprake is van verwerking van persoonsgegevens. Gegevens met betrekking tot het e-mail- en internetgebruik 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 of politieke ambtsdrager. 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 AVG hanteert een ruime definitie voor het begrip ‘verwerking’: het gehele proces van verzamelen tot aan vernietigen van gegevens.

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: ambtenaren en personen die (betaald of niet-betaald) werkzaamheden voor de gemeente verrichten, anders dan in ambtelijk dienstverband. Daarnaast geldt het privacyreglement ook voor politieke ambtsdragers (zijnde collegeleden).

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, zullen de regels in dit privacyreglement van overeenkomstige toepassing zijn. 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 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 Doeleinden

De AVG bepaalt, dat gegevens op een behoorlijke, rechtmatige en transparante wijze moeten worden verwerkt (artikel 5, lid 1, sub a AVG). Dit voorschrift geldt in zoverre als de privacyrechtelijke evenknie van de arbeidsrechtelijke norm van goed werkgeverschap. Persoonsgegevens mogen voorts slechts voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verwerkt (artikel 5, lid 1, sub b AVG). 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 6, lid 1, sub f AVG). 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 c.q. politieke ambtsdrager dan strikt noodzakelijk is (subsidiariteit). In het privacyreglement zijn vier doeleinden geformuleerd.

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 hebben bepaald 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 beheerders 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 Security Officer dient tegenover het management een zekere onafhankelijkheid te hebben. Er moet dus een heldere procedure te bestaan over wie in welke gevallen de Security Officer 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 4, vierde lid
De verwerkingsverantwoordelijke dient het recht op privacy van een (ex)-medewerker of (ex)-politieke ambtsdrager te respecteren. Het lezen van privé-mail van een (ex)-medewerker of (ex)-politieke ambtsdrager is, behoudens bijzondere omstandigheden, niet toegestaan. Bij uitdiensttreding c.q. ontslag

is de medewerker zelf verantwoordelijk voor het verwijderen van privé-berichten uit de mailbox of bestanden. De politieke ambtsdrager is bij beëindiging van zijn/haar functie ook zelf verantwoordelijk voor het verwijderen van privé-berichten uit de mailbox of bestanden.
Artikel 4, vijfde en zesde lid
Het is ingeval van uitdiensttreding, langdurige ziekte van een medewerker en noodsituaties van belang dat de continuïteit van de bedrijfsvoering en de dienstverlening geborgd is. Ten behoeve van het bedrijfsbelang kan het noodzakelijk zijn om toegang tot de mailbox of bestanden te krijgen.
Bij uitdiensttreding en ontslag kan een analyse van de mailbox of bestanden plaatsvinden, zodat belangrijke mail of bestanden niet verloren gaat. Tevens kan dit van belang zijn in het kader van de opvolging van de ex-medewerker.
In bovenstaande gevallen wordt rekening gehouden met de privacy-belangen van de (ex)-medewerker en de geldende normen omtrent kennisneming van privé-mail / bestanden.

Artikel 5 Gebruik elektronische communicatiemiddelen

In dit artikel van het Privacyreglement zijn gedragsregels opgenomen over wat er in de organisatie onder verantwoord e-mail- en internetgebruik wordt verstaan.

Een totaal verbod van privé-gebruik van de elektronische communicatiemiddelen is 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). Er kunnen wel beperkende voorwaarden worden gesteld aan het persoonlijk gebruik van de elektronische communicatiemiddelen.

Artikel 6 Controle

In dit artikel wordt aangegeven aan wie binnen de organisatie overzichten worden verstrekt in verband met de diverse doeleinden van de gegevensverwerking.

Bijvoorbeeld in verband met het doeleinde in artikel 3, onder a het volgende opnemen: 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.

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 de gemeente inzicht wil hebben in de meest bezochte internetsites, bijvoorbeeld in de vorm van een top tien. Daarvoor zal wel kennisgenomen dienen te worden van inhoudelijke gegevens.
Artikel 6, eerste lid, onder sub b
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.

De gemeente gaat gebruik maken van content filtering (zie hieronder) om te waarborgen dat informatie die voldoet aan de criteria zoals vastgelegd in de richtlijnen Informatiebeveiliging van de gemeente, niet buiten de organisatie op oneigenlijke wijze gebruikt kan worden. Het filter zal in beginsel geen inbreuk maken op persoonsgegevens maar slechts op de content en niet op de afzender. De maatregelen (en de afhandeling hiervan) voor controle van content en betrokken werknemer zijn gelijkgesteld aan de regels van dit Privacyreglement.

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:

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
Bewijs en archivering: conform het bepaalde in artikel 6, lid 3 (goedkeuring gemeentesecretaris) maakt de Security Officer in samenwerking met de dienstverlener (medio 2014 is dat Fujitsu) een kopie van de zakelijke e-mailberichten met als doel bewijs en/of archivering.

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

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:

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. Controle op de inhoud vindt slechts plaats na goedkeuring door de gemeentesecretaris.

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.
Om te waarborgen, dat er niet te gemakkelijk wordt geoordeeld dat er zwaarwegende redenen zijn, is opgenomen dat de gemeentesecretaris in dat geval tevoren goedkeuring moet verlenen. Dat inhoudelijke overzicht kan naar de betreffende afdelingsmanager (of hoger kader) worden gestuurd.

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
In het vijfde lid is opgenomen:

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

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.

Artikel 6, zesde en zevende lid
In het zesde lid is opgenomen:

Het gebruik van de elektronische communicatiemiddelen door bijvoorbeeld OR-leden, GO-leden, mediators, bedrijfsartsen, andere medewerkers met een vertrouwensfunctie en politieke ambtsdragers 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 Landelijk Overleg Gemeentelijke Arbeidsvoorwaarden (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 van de Collectieve arbeidsvoorwaardenregeling en Uitwerkingsovereenkomst (CAR-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. Naar het oordeel van het AP geldt artikel 6, zesde lid niet alleen voor het gebruik van e-mailfaciliteiten, maar ook voor internetgebruik.

Tussen de collegeleden en de verwerkingsverantwoordelijke bestaat geen gezagsrelatie. De verwerkingsverantwoordelijke kan zijn gezagsbevoegdheid dus niet aanwenden om het e-mail-, internetgebruik van de politieke ambtsdragers te controleren. Het betreft hier geen absoluut verbod. Er kan van worden afgeweken in bepaalde situaties waarbij de het Privacyreglement wordt overtreden. In het kader van de bestuurlijke integriteit is, gelet op het bepaalde in artikel 170, lid 2 van de Gemeentewet, in dit verband een rol voor de burgemeester weggelegd.
Controle in het kader van het beveiligen van het systeem en netwerk vindt wel (op geautomatiseerde wijze) plaats.

Artikel 7 Bewaring en verwijdering

Bij bewaring en verwijdering wordt door gemeente rekening gehouden met de archiefwet.

Artikel 7, eerste lid
Het eerste lid is geherformuleerd.

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.

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 c.q. politieke ambtsdrager noodzakelijk is. Zodra een nader onderzoek is afgerond en dit niet leidt tot maatregelen jegens een medewerker c.q. politieke ambtsdrager worden de gegevens verwijderd.

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 en politieke ambtsdragers

In artikel 8 worden de rechten van de medewerkers en politieke ambtsdragers bij het verwerken van persoonsgegevens behandeld. Transparantie is een belangrijk beginsel voor privacybescherming. De informatieplicht is gebaseerd op de artikelen 13 en 14 AVG. Daarnaast hebben de medewerkers en politieke ambtsdragers een inzage- en rectificatierecht.

Artikel 9 Sancties

Er is een splitsing gemaakt tussen drie categorieën. Namelijk werknemers in dienst van de gemeente, personen die (betaalde of niet betaalde) werkzaamheden voor de gemeente verrichten en politieke ambtsdragers. Het eerste lid is opnieuw geformuleerd waarbij ontslag als disciplinaire straf expliciet wordt genoemd.
Het eerste lid is geherformuleerd:

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.

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

Ten aanzien van politieke ambtsdragers wordt verwezen naar de sanctiemogelijkheden die in de Gedragscode integriteit burgemeester en wethouders gemeente Almere 2016 worden genoemd.

Artikel 10 Onvoorziene omstandigheden

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

Artikel 11 Openbaarmaking, inwerkingtreding en evaluatie

Het Privacyreglement dient helder naar de medewerkers en politieke ambtsdragers te worden gecommuniceerd. De medewerkers en politieke ambtsdragers 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 en politieke ambtsdragers worden gepresenteerd tijdens het opstarten van het systeem of van het programma. Op die manier is verzekerd dat de men zich bewust is van het Privacyreglement.

In het derde lid is opgenomen:

3. Dit Privacyreglement wordt vierjaarlijks geëvalueerd door de verwerkingsverantwoordelijke en de Ondernemingsraad..

Regels verouderen omdat de organisatie, de omgeving waarin zij verkeert en de technische mogelijkheden wijzigen. Het is dan ook zaak periodiek de regels te evalueren opdat tijdig eventuele bijstelling kan plaatsvinden.

Artikel 12 Slotbepaling

Elektronische controle van computergebruik raakt het terrein van de bescherming van de persoonlijke levenssfeer van de gebruiker. Op het controleren van het gebruik van e-mail en internet op de werkplek is daarom de AVG van toepassing.