Regeling ICT-gebruik 2011

Inhoud:

1. Definities, reikwijdte en doeleinden
2. Verantwoordelijkheden en beheer
3. Gebruik elektronische communicatiemiddelen
4. Vastlegging, bewaring, verwijdering en verstrekking van persoonsgegevens
5. Rechten van betrokkene: verbeteren, aanvullen, verwijderen of afschermen van persoonsgegevens
6. Sancties, openbaarmaking, inwerkingtreding en slotbepaling

---

HOOFDSTUK 1: DEFINITIES, REIKWIJDTE EN DOELEINDEN

Artikel 1 Definities

In de Regeling ICT-gebruik 2011 wordt verstaan onder:

1. medewerker:
   a. ambtenaar volgens artikel 1:1 lid 1 sub a, en artikel 1:2 sub a en d van de CAR/UWO en
   b. degene die op arbeidsovereenkomst of anderszins betaalde of onbetaalde werkzaamheden voor de gemeente verricht;

   die gebruiker is van ICT-middelen waarin persoonsgegevens staan;

2. ICT-middelen: alle huidige en toekomstige elektronische communicatie middelen en ICT-apparatuur, door of namens de gemeente aan de medewerkers beschikbaar gesteld;

3. Elektronische communicatiemiddelen: e-mail-, internet- en telefoonfaciliteiten;

4. ICT-apparatuur: elektronische informatie- en communicatiemiddelen, inclusief alle bijbehorende hard- en software en bestanden;
5. Privébestand: bestand met een geheel of overwegend persoonlijke inhoud;
6. Persoonsgegeven: elk gegeven met een geïdentificeerde of identificeerbare natuurlijke persoon in de zin van de Wet bescherming persoonsgegevens;
7. Verwerken van persoonsgegevens: elke handeling of elk geheel van handelingen met persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken waaronder ook doorzending, verspreiding of enige andere vorm van het beschikbaar stellen, samenbrengen, met elkaar in verband brengen, en het afschermen, uitwissen of vernietigen van gegevens vallen;
8. Verkeersgegevens: gegevens die worden verwerkt voor het overbrengen van communicatie over een elektronisch communicatienetwerk of voor de facturering ervan;

9. Bestand: elk, al dan niet geautomatiseerd, gestructureerd geheel van persoonsgegevens, ongeacht of dit geheel van gegevens gecentraliseerd is of verspreid is op een functioneel of geografisch bepaalde wijze, dat volgens bepaalde criteria toegankelijk is en gaat over verschillende personen;
10. Verantwoordelijke: het college van burgemeester en wethouders van de gemeente Zoetermeer, als bestuursorgaan dat het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt;
11. Onrechtmatig gebruik en misbruik van de ICT-middelen: een doen of nalaten in strijd met deze regeling of andere wet- of regelgeving.

Artikel 2 Reikwijdte

1. Deze regeling is voor alle medewerkers van toepassing bij het gebruik van ICT-middelen en de wijze waarop controle hierop plaatsvindt. Ook is deze regeling van toepassing op het verwerken van persoonsgegevens.

Artikel 3 Doeleinden

1. De verwerking van persoonsgegevens door het gebruik van de elektronische communicatiemiddelen heeft de volgende doeleinden:

    a. het verkrijgen van inzicht in de aard en mate van gebruik van de ICT-middelen;
    b. het voorkomen van onrechtmatig gebruik en/of misbruik van de ICT-middelen;
    c. het beveiligen van het systeem en het netwerk;
    d. het beschermen van de privacy van de medewerkers op de werkplek;
    e. het beschermen van de integriteit en goede naam van de gemeente;
    f. het beheer van de ICT-middelen.

2. De omvang van de controle om onrechtmatig gebruik te voorkomen en/of misbruik van de ICT-middelen zoals in het eerste lid onder sub b, wordt zo beperkt mogelijk gehouden. De controle moet in een redelijke verhouding staan tot de geformuleerde doeleinden.

HOOFDSTUK 2: VERANTWOORDELIJKHEDEN EN BEHEER

Artikel 4 Verantwoordelijkheden en beheer

1. De verantwoordelijke treft de nodige maatregelen, zodat persoonsgegevens juist, nauwkeurig en volgens de doeleinden worden verwerkt.
2. De verantwoordelijke treft passende technische en organisatorische maatregelen om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking.
3. De verantwoordelijke wijst een of meerdere systeembeheerders aan die zorgen voor het beheer van het (de) bestand(en). Deze systeembeheerders zijn, op grond van art. 125a, derde lid, Ambtenarenwet, verplicht tot geheimhouding van de verkregen persoonsgegevens, behalve als zij door een

wettelijke voorschrift tot mededeling zijn verplicht of uit hun taak de noodzaak tot mededeling blijkt.

HOOFDSTUK 3: GEBRUIK ICT-MIDDELEN

Artikel 5 Gebruik ICT-middelen

1. Medewerkers gebruiken de ICT-middelen hoofdzakelijk voor het uitvoeren van de gemeentelijke werkzaamheden.
2. Het is medewerkers verboden om de ICT-middelen aan een ander ter beschikking te stellen. Dit verbod geldt niet voor het tijdelijk laten gebruiken van de ICT-middelen door een andere medewerker.
3. Incidenteel privégebruik van de ICT-middelen door medewerkers is toegestaan als dit gebruik in overeenstemming is met deze regeling en dit gebruik niet storend is en/of ten koste gaat van het uitvoeren van de gemeentelijke werkzaamheden.
4. Het is medewerkers niet toegestaan om de ICT-middelen te gebruiken voor het opvragen, versturen, vastleggen of anderszins verwerken van pornografisch, erotisch, racistisch materiaal of informatie die als lasterlijk, beledigend, aanstootgevend of oneervol wordt beschouwd; het meedoen aan chatsessies, online te gokken of te gamen, kettingbrieven te versturen illegale software, films of muziek te downloaden en betaaldiensten af te nemen. Ook is het niet toegestaan om zonder voorafgaand overleg met de systeembeheerder(s) bestanden te verzenden of op te vragen waarvan de medewerkers redelijkerwijs moet aannemen dat deze te omvangrijk zijn of een elektronisch bericht aan alle of vrijwel alle medewerkers van de gemeente tegelijkertijd te versturen.
5. .
6. Medewerkers waarborgen bij het gebruik van de ICT-middelen de integriteit en goede naam van de gemeente Zoetermeer..
7. .
8. .
9. .
10. Medewerkers werken op basis van de gestelde beveiligingseisen van de ICT-middelen en informatie. Bij vertrouwelijke of persoonsinformatie treffen de medewerkers voorzorgsmaatregelen, zoals afscherming van wachtwoord en/of het gebruik van speciale programmatuur voor de toepassing van encryptie.
11. Medewerkers moeten schade aan, verlies of diefstal van ICT-middelen gelijk bij de leidinggevende melden.

Artikel 6 Controle

1. Controle door of in opdracht van de (algemeen) directeur op het gebruik van de ICT-middelen vindt alleen plaats voor de in artikel 3 genoemde doeleinden. Deze doeleinden stellen beperkingen aan de omvang en wijze van controle.

a. Controle om inzicht te krijgen in de mate van gebruik van de ICT-middelen wordt beperkt tot de verkeersgegevens, die gaan over tijd, hoeveelheid, omvang en dergelijke.
b. Controle om onrechtmatig gebruik en misbruik van de ICT-middelen te voorkomen wordt zo beperkt mogelijk gehouden, zodat ze in redelijke verhouding staat tot het doel waarvoor ze worden gebruikt. Bovendien vindt de controle in eerste instantie geanonimiseerd en slechts steekproefsgewijs plaats.
c. Controle voor de beveiliging van het systeem en het netwerk zoals het tegengaan van virussen en andere schadelijke programma's vindt op geautomatiseerde wijze plaats.

2. Controle vindt in eerste instantie plaats op het niveau van getotaliseerde gegevens die niet herleidbaar zijn tot individuele personen.
   Indien een medewerker wordt verdacht van het overtreden van deze regeling, kan gedurende een vastgestelde periode gerichte controle plaatsvinden.
   Deze gerichte controle wordt slechts uitgevoerd nadat de medewerker is ingelicht dat signalen hierover zijn ontvangen en om zijn reactie is gevraagd. De (algemeen) directeur kan deze inlichtingenplicht buiten beschouwing laten voor zover dit noodzakelijk is voor de in artikel 43 van de Wet bescherming persoonsgegevens genoemde belangen. In dit geval worden betrokkenen altijd wel zo spoedig mogelijk geïnformeerd over de gerichte controle.
3. Controle beperkt zich tot verkeersgegevens van het gebruik van de ICT-middelen, tenzij sprake is van zwaarwegende redenen. Alleen bij zwaarwegende redenen kan er controle op de inhoud plaatsvinden.
   Privébestanden worden hierbij zoveel mogelijk ontzien.
4. Onrechtmatig gebruik dan wel misbruik van de ICT-middelen wordt zo veel mogelijk softwarematig onmogelijk gemaakt.
5. De in lid 1 en lid 2 van dit artikel genoemde controles kunnen ook plaatsvinden door de directeur Bedrijfsvoering voor het in artikel 3 onder f genoemde beheer van de ICT-middelen.
6. Als geconstateerd wordt dat een medewerker zich niet houdt aan de bepalingen van deze regeling, wordt de betrokken medewerker zo spoedig mogelijk hierop aangesproken door zijn leidinggevende.

HOOFDSTUK 4: VASTLEGGING, BEWARING, VERWIJDERING EN VERSTREKKING VAN PERSOONSGEGEVENS

Artikel 7 Vastlegging persoonsgegevens

In de in artikel 6 genoemde gerichte controle worden ten hoogste de volgende persoonsgegevens vastgelegd:

a. gebruikersidentificatie, naam, voornaam of voorletters van de medewerker;
b. naam en/of codering van de sector, afdeling waaronder de medewerker valt;
c. gegevens over de toegang tot internet die door de gemeente is geboden aan de medewerker, inclusief gebruikersnaam en internet protocoladres;

d. gegevens over de datum en het tijdstip van het openen en sluiten van de toegang tot internet door de medewerker en gegevens over de datum en het tijdstip van het verzenden, en het ontvangen van e-mailberichten door de medewerker;
e. gegevens, inclusief datum en tijdstip, van de door de medewerker bezochte internetsites (internet protocoladressen en (de onderdelen van) de webpagina's);
f. de inhoud van de door de medewerker verzonden en ontvangen e-mailberichten.

Artikel 8 Bewaring en verwijdering

1. De in artikel 7 genoemde persoonsgegevens worden maximaal zes maanden bewaard. Gegevens die ouder zijn dan zes maanden worden automatisch verwijderd, tenzij er een redelijk vermoeden bestaat van onrechtmatig gebruik en/of misbruik van de ICT-middelen in die periode. In dat geval worden de gegevens bewaard zolang dit in het kader van nader onderzoek en eventueel te treffen maatregelen tegen de medewerker noodzakelijk is. Zodra een nader onderzoek is afgerond en dit niet leidt tot maatregelen tegen de medewerker worden de gegevens verwijderd.
2. Indien de systeembeheerder om technische redenen persoonsgegevens als bedoeld in artikel 8, eerste lid, niet kan verwijderen, wordt onder verwijderen verstaan het niet meer verstrekken van deze gegevens voor de in artikel 3 geformuleerde doeleinden.

Artikel 9 Personen aan wie (persoons)gegevens worden verstrekt

1. Om inzicht te verkrijgen in de mate van gebruik van de ICT-middelen worden getotaliseerde gegevens die niet herleidbaar zijn tot individuele personen verstrekt aan de I-controller.

2. Als daartoe aanleiding bestaat bespreekt de I-controller de overzichten met de leidinggevende.

3. De leidinggevende kan als sprake is van een redelijk vermoeden van onrechtmatig gebruik of misbruik van de ICT-middelen op basis van artikel 6, lid 2 de systeembeheerder opdracht geven bij een bepaalde medewerker voor een aangegeven periode een omschreven controle op het gebruik van de ICT-middelen uit te voeren. De systeembeheerder brengt over deze controle direct rapport uit aan de leidinggevende van de medewerker.

HOOFDSTUK 5: RECHTEN VAN DE MEDEWERKER: VERBETEREN, AANVULLEN, VERWIJDEREN OF AFSCHERMEN VAN PERSOONSGEGEVENS

Artikel 10 Rechten van de medewerker

1. De medewerker heeft het recht om een kopie van een overzicht te ontvangen van de hem betreffende persoonsgegevens die worden verwerkt. De

medewerker kan hiervoor een schriftelijk verzoek indienen bij het college van burgemeester en wethouders.

2. Als de betreffende persoonsgegevens feitelijk onjuist, voor het doel of de doeleinden van de verwerking onvolledig of niet relevant zijn, of in strijd zijn met een wettelijk voorschrift, kan de medewerker het college schriftelijk verzoeken deze gegevens te verbeteren, aan te vullen, te verwijderen of af te schermen. Het verzoek bevat de aan te brengen wijzigingen.
3. Het college van burgemeester en wethouders bericht de medewerker binnen vier weken na ontvangst van het in het tweede lid genoemde verzoek schriftelijk of, 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, OPENBAARMAKING, INWERKINGTREDING EN SLOTBEPALING

Artikel 11 Sancties

1. Medewerkers, die ambtenaar zijn en deze regeling niet naleven, kunnen disciplinair worden bestraft op basis van de arbeidsvoorwaarden van de gemeente.
2. Medewerkers die geen ambtenaar zijn en deze regeling niet naleven, mogen al dan niet tijdelijk, geen ICT-middelen gebruiken of kan de gemeente de contractuele relatie mee verbreken.

Artikel 12 Onvoorziene omstandigheden

In gevallen waarin deze regeling niet voorziet of bij twijfel over de toepassing van deze regeling beslist de verantwoordelijke.

Artikel 13 Openbaarmaking

Deze regeling wordt verstrekt aan of is te raadplegen door degenen die, direct of indirect, de beschikking krijgen over ICT-middelen.

Artikel 14 Wet bescherming persoonsgegevens

Onverminderd het bepaalde in deze regeling, is de Wet bescherming persoonsgegevens van toepassing op het verwerken van persoonsgegevens.

Artikel 15 Intrekking oude regeling

Het Privacyreglement e-mail en internetgebruik van 16 december 2003 wordt ingetrokken.

Slotbepalingen

De regeling genaamd: “Regeling ICT-gebruik 2011”treedt in werking op de dag na de bekendmaking op Intranet.

Vastgesteld in het college van burgemeester en wethouders van 2011.

Toelichting regeling ICT-gebruik 2011

Algemeen

De regeling ICT-gebruik 2011 vervangt de Nettiquette, de regels voor e-mail en internetgebruik en breidt deze tegelijk uit tot een regeling voor alle communicatiefaciliteiten (dus bijv. ook telefoon) en alle denkbare ICT- apparatuur, inclusief software en bestanden.
Dus kortweg een regeling voor alle ICT-gebruik (gebruik van informatie- en communicatietechnologie).

De regeling stelt regels:

- waaraan het ICT-gebruik dient te voldoen (zorgvuldigheid, zakelijk gebruik, beveiliging en vermijden ongewenst gebruik en misbruik) en
- hoe controle op dat gebruik kan plaatsvinden;
- over het verwerken van persoonsgegevens bij het ICT-gebruik en de controle daarop (privacy) en
- over sancties.

De voorwaarden waaraan het gebruik dient te voldoen zijn in feite voorwaarden die de gemeente Zoetermeer stelt bij het verstrekken van de ICT-middelen aan de medewerkers.

De controles hebben verschillende doeleinden. Het gaat om handhaving van de gebruiksregels, de bedrijfsvoering en om de bescherming van de integriteit en goede naam van de gemeente Zoetermeer.

De waarborging van de privacy in deze regeling voldoet aan de eisen die het college bescherming persoonsgegevens (dit is het toezichthoudend orgaan voor de privacy) stelt bij de verwerking en controles van persoonsgegevens.
Registratie van ICT-gebruik, inclusief de controlemogelijkheden, vindt veelal automatisch en daardoor onmerkbaar plaats. Dit is een mogelijke bedreiging van de privacy. Er moet dus duidelijk zijn wat wel en wat niet mag en welke rechten medewerkers hebben.

Sancties worden vermeld omdat vooraf helder moet zijn dat de gemeente Zoetermeer dit onderwerp serieus neemt en indien de omstandigheden daartoe aanleiding geven, ook streng zal optreden.
Vooral vanwege dat laatste is duidelijkheid over de gebruiksregels vereist.

Artikelsgewijze toelichting

Artikel 1 Begripsbepalingen
De begrippen die in de Regeling ICT-gebruik 2011 voorkomen, worden in dit artikel gedefinieerd. Voor de omschrijving van de begrippen is waar mogelijk aangesloten bij de bewoordingen van de Wet bescherming persoonsgegevens (Wbp).
Deze wet is van toepassing bij de verwerking van persoonsgegevens. Gegevens over het ICT-gebruik van medewerkers zijn persoonsgegevens.

Artikel 2 Reikwijdte
In dit artikel wordt geregeld dat de regeling van toepassing is op alle medewerkers die werkzaam zijn bij de gemeente Zoetermeer. De rechtsverhouding tussen hen en de werkgever is hierbij niet relevant. Zo hebben bijvoorbeeld ook uitzendkrachten, externe adviseurs en andere medewerkers die een tijdelijk contract met de gemeente Zoetermeer zijn aangegaan, zich te houden aan deze regeling.

Artikel 3 Doeleinden
Om privacy te waarborgen is het noodzakelijk om de doelen van het verwerken van persoonsgegevens en het uitvoeren van controles vooraf vast te stellen.
Met dit artikel wordt aan deze eisen voldaan.
Deze doeleinden moeten wel een wettelijke grondslag hebben (artikel 8 van de Wet bescherming persoonsgegevens). Er is sprake van een gerechtvaardigd belang van de gemeente. Dit geldt voor alle hier genoemde doelen. De privacybelangen van de medewerkers moeten wel meegewogen worden.
De doelen zijn verder van belang voor het beoordelen van de proportionaliteit en subsidiariteit van de inbreuk op de privacy. Dit betekent dat:

- de aard, omvang en vorm van de verwerking en de controlemaatregelen in een redelijke verhouding tot de genoemde doelen moet staan;
- de verwerking van persoonsgegevens en de controles mogen niet méér inbreuk maken op de belangen van de medewerker dan strikt noodzakelijk is.

Artikel 4 Verantwoordelijkheden en beheer
Het beheer van ICT-middelen, het gebruik van communicatiefaciliteiten, controles, etc. brengen allerlei verwerkingen van persoonsgegevens met zich mee.

Privacy-consequenties zijn dat:

- maatregelen nodig zijn om ervoor te zorgen dat deze persoonsgegevens juist en nauwkeurig zijn (lid 1);
- deze persoonsgegevens beveiligd worden (lid 2);
- beperkte toegang en geheimhouding wordt gerealiseerd (lid 3);
- vanwege de enorme hoeveelheid informatie die geautomatiseerd wordt verwerkt, zijn het vooral de geautomatiseerde verwerkingen die hierin aandacht vragen, denk bijvoorbeeld aan alle bezochte internetadressen die worden vastgelegd of de telefoonregistratie die alle telefoonnummers bevat.

In eerste aanleg gaat het alleen om verkeersgegevens (dus welke IP adressen van computers of telefoonnummers), maar koppeling van deze verkeersgegevens aan

een persoon is een mogelijkheid. Zodra dit laatste het geval is worden de eisen van dit artikel van belang voor de bescherming van de privacy.

Artikel 4, eerste lid - juist en nauwkeurig
Met de “nodige” maatregelen wordt bedoeld dat alle maatregelen moeten worden getroffen die in redelijkheid kunnen worden gevergd. Wat redelijk is wordt in samenhang bepaald door:

- de soort gegevens die worden verwerkt (bijzondere gegevens vragen om meer aandacht);
- de stand van de techniek;
- de kosten/benodigde inspanning van de maatregelen.

Artikel 4, tweede lid - beveiligen
De beveiligingsmaatregelen garanderen, rekening houdend met de stand van de techniek en de uitvoeringskosten, een passend beveiligingsniveau.
Wat passend is, is afhankelijk van de risico’s van de verwerking en de aard van de te beschermen gegevens.
De maatregelen zijn er ook op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen.

Artikel 4, derde lid - geheimhouding
Een of meer systeembeheerders zijn met het beheer van de bestanden belast. Deze medewerkers hebben uit hoofde van hun functie toegang tot alle gegevens in het computernetwerk. Deze functie moet met de nodige waarborgen worden omgeven. De systeembeheerder moet zich ervan bewust zijn dat hij gegevens die hij tijdens het werk tegenkomt, geheim moet houden. De enige uitzondering hierop is als een wettelijk voorschrift hem tot mededeling verplicht of uit de taak de noodzaak tot mededeling volgt.
De systeembeheerder is uiteraard niet bevoegd tot het lezen van documenten of e-mail of het meekijken met het internetgebruik van de medewerkers. De systeembeheerder moet tegenover het management een zekere onafhankelijkheid hebben. Er moet dus binnen de gemeente Zoetermeer een heldere procedure zijn over wie in welke gevallen de systeembeheerder opdracht kan geven om bepaalde zaken op het netwerk nader te controleren of daarover informatie te verschaffen. Artikel 6 is hiervoor het kader.

Artikel 5 Gebruik elektronische communicatiemiddelen
De ICT-middelen zijn eigendom van de gemeente Zoetermeer en worden verstrekt voor het uitvoeren van de werkzaamheden. De werkgever kan op basis van zijn gezagsbevoegdheid voorwaarden stellen aan het gebruik van ICT-middelen of bepaalde soorten gebruik verbieden.

Voor de hand ligt, dat de eerste voorwaarde is dat de ICT-middelen moeten worden gebruikt voor het uitvoeren van de werkzaamheden. Daar zijn ze immers ook (uitsluitend) voor verstrekt.
Het verbod om de middelen door een ander te laten gebruiken geldt zowel voor betaalde als onbetaalde verstrekking. Het is vanzelfsprekend wel toegestaan om de telefoon of dergelijke even te laten gebruiken door een collega.

Lid 3 geeft aan dat incidenteel privégebruik is toegestaan. Dit gebruik mag echter niet ten koste gaan van de dagelijkse werkzaamheden.
Uitgangspunt blijft het (100%) zakelijk gebruik van het eerste lid. Dit geldt vooral voor de werkplek.
Het is echter incidenteel wel eens noodzakelijk om op de werkplek privézaken te regelen. Dit is daarom ook toegestaan.

Het vierde lid omschrijft het ongewenst gebruik. Dit is geen uitputtende opsomming. In een enkel geval is het denkbaar dat dergelijk gebruik functioneel is voor bijvoorbeeld beleidsvoorbereidend onderzoek.
In dat geval is het noodzakelijk dit vooraf met de leidinggevende te bespreken.

Waar het vierde lid vooral ziet op de inhoud van de – ongewenste – informatie, ziet het vijfde lid vooral op risico's en belasting van het netwerk.

De zorgvuldigheid en integriteit van de gemeente van het zesde lid zijn de kernbegrippen van het gebruik. De boodschap is eenvoudig en veelomvattend: ga zorgvuldig om met de ICT-middelen en informatie van de gemeente. Deze zorgvuldigheid is vergelijkbaar met begrippen als goed werknemer en goed huisvader.

Lid 7 ziet in de eerste plaats op de beveiliging van de ICT-apparatuur, netwerk en systemen. Dit gaat veelal om reeds genomen maatregelen, die gerespecteerd moeten worden.
Verder gaat dit zevende lid over de beveiliging van vertrouwelijke en geheime informatie. Vertrouwelijk is die informatie die niet (algemeen) bekend mag worden. Geheim is vertrouwelijke informatie die als geheim is bestempeld.
Het gaat hier om die informatie waarvan de medewerker weet of redelijkerwijs moet weten dat deze vertrouwelijk of geheim is. Voorbeelden zijn financiële- en persoonsinformatie. Vereist zijn hierbij maatregelen die waarborgen dat alleen geautoriseerden toegang krijgen en dat informatie niet kan uitlekken. Voorbeelden zijn het gebruik van encryptie of wachtwoorden of het gebruik van een beveiligde usb-stick.
Het meteen melden van schade, verlies en diefstal zorgt ervoor dat zo snel mogelijk maatregelen genomen kunnen worden. De leidinggevende meldt dit vervolgens aan de beheerorganisatie.

Artikel 6 Controles

Artikel 6, eerste lid, onder a
Om inzicht te verkrijgen in de mate van het gebruik van de ICT-middelen, kan in het kader van kosten- en capaciteitsbeheersing, de controle beperkt blijven tot verkeersgegevens (tijd, hoeveelheid, omvang en dergelijke). Kennisneming van de inhoud is dan niet noodzakelijk.

Artikel 6, eerste lid, onder b
De genomen maatregelen moeten in redelijke verhouding staan tot de belangen van de medewerker en de gebruikte middelen mogen niet een verdergaande inbreuk maken op die belangen dan strikt noodzakelijk (proportionaliteit en subsidiariteit). Steeds zal hiertoe een belangenafweging moeten plaatsvinden. Het doel

rechtvaardigt dus niet een continue controle en daarmee gepaard gaande verregaande inbreuk op de persoonlijke levenssfeer van de medewerker. In eerste instantie vindt de controle op naleving slechts steekproefsgewijs en geanonimiseerd plaats.

Artikel 6, eerste lid, onder c
Vanuit beveiligingsoogpunt is het wenselijk om internet- en e-mailgebruik 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 tussen zakelijke en privé e-mail.

Artikel 6, tweede lid
Het is in het algemeen niet noodzakelijk om de (algemeen) directeur rapportages en gebruiksstatistieken van het ICT-gebruik van de medewerkers op persoonsniveau te verstrekken. De gegevens in de rapportages en statistieken kunnen dus meestal ontdaan worden van hun identificerende kenmerken. Alleen als er concrete verdenkingen bestaan tegen een bepaalde medewerker, is rapportage op persoonsniveau noodzakelijk en toegestaan. Bij een gerichte controle, dient de betrokken medewerker vooraf te worden geïnformeerd en om zijn reactie gevraagd. Deze informatieplicht kan worden opgeschort voor zover dit noodzakelijk is is in het belang van:

a. de veiligheid van de staat;
b. de voorkoming, opsporing en vervolging van strafbare feiten;
c. gewichtige economische en financiële belangen van de staat en andere openbare lichamen;
d. het toezicht op de naleving van wettelijke voorschriften die zijn gesteld ten behoeve van de belangen, bedoeld onder *b* en *c*, of
e. de bescherming van de betrokkene of van de rechten en vrijheden van anderen (de verantwoordelijke daaronder begrepen).

De mogelijkheid tot opschorting van de informatieplicht geldt ook voor zover dat noodzakelijk is voor de voorkoming, opsporing en vervolging van ernstig plichtsverzuim. (zie onder e: het belang van de rechten van de gemeente).
Het noodzakelijkheidvereiste dwingt tot een expliciete afweging als niet vooraf wordt geïnformeerd. In dat geval moet altijd wel alsnog achteraf worden geïnformeerd dat een onderzoek heeft plaatsgevonden.

Artikel 6, derde lid
In principe is de controle van elektronische communicatiemiddelen beperkt tot de verkeersgegevens. Dit zijn gegevens met betrekking tot datum, tijd, hoeveelheid en omvang. Slechts bij *zwaarwegende* redenen wordt inhoudelijk gecontroleerd.

Artikel 6, vierde lid
Onrechtmatig gebruik en/of misbruik van de elektronische communicatiemiddelen kan in sommige gevallen via geïnstalleerde software worden voorkomen, bijvoorbeeld 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.
Deze content filtering wordt binnen de gemeente toegepast.

Artikel 6, vijfde lid
Controles vinden plaats in opdracht van de (algemeen) directeur waar de medewerker werkzaam is. Voor het beheer van de ICT-middelen kan ook de directeur Bedrijfsvoering opdracht geven voor controleactiviteiten op de ICT-middelen waarover hij het beheer voert. Dit zal echter nooit de inhoud van communicatie of bestanden betreffen.

Artikel 6, zesde lid
Een bepaalde tijd voor de opbouw van het dossier is toegestaan als de omstandigheden daartoe aanleiding geven. Als de medewerker op zijn handelen in strijd met de regeling wordt aangesproken, is het raadzaam dat hij gewaarschuwd wordt voor de (rechtspositionele) gevolgen bij voortzetting van dit gedrag.

Artikel 7 Vastlegging persoonsgegevens
In dit artikel wordt aangegeven welke persoonsgegevens worden vastgelegd.

Artikel 8 Bewaring en verwijdering

Artikel 8, eerste lid
Het is in het algemeen niet nodig om de persoonsgegevens lang te bewaren. De standaardtermijn is zes maanden. In het geval van een zwaarwegend vermoeden van onrechtmatig gebruik en/of misbruik van ICT-middelen, worden de gegevens bewaard, zolang dit in het kader van nader onderzoek en eventueel te treffen maatregelen tegen een medewerker noodzakelijk is. Zodra een nader onderzoek is afgerond en dit niet leidt tot maatregelen tegen een medewerker 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 back-up een individueel e-mailbericht te verwijderen. De bedoelde gegevens mogen in deze gevallen niet meer worden verstrekt (verwerkt).

Artikel 9 Personen aan wie (persoons)gegevens worden verstrekt

Artikel 1
Inzicht in de mate van gebruik van ICT middelen worden in getotaliseerde gegevens, die niet herleidbaar zijn tot individuele personen aangeleverd bij de I-controller. De I-controller heeft deze verkeersgegevens nodig voor de uitoefening van zijn functie.

Artikel 2
Als de verkeersgegevens hiervoor aanleiding geven dan bespreekt de I-controller dat met de leidinggevende, zodat de gegevens verklaard kunnen worden.

Artikel 3
De leidinggevende is verantwoordelijk voor het personeel en kan aan de systeembeheerder opdracht geven om een gerichte controle uit te voeren op het gebruik van ICT-middelen door een bepaalde medewerker.

Artikel 10 Rechten van de medewerker
In dit artikel worden de rechten van de medewerkers bij het verwerken van persoonsgegevens omschreven.
Het eerste lid geeft het recht op inzage weer. Dit recht is geregeld in artikel 35 van de Wet bescherming persoonsgegevens (Wbp).
Het verzoek tot aanvullen, verbeteren, verwijderen of afschermen van de gegevens kan alleen plaatsvinden als daarvoor een feitelijke reden is. Dit is omschreven in het tweede lid en is vastgelegd in artikel 36 van de Wbp.
De in het derde lid genoemde motivering is nodig omdat een weigering een besluit in de zin van de Algemene wet bestuursrecht is.
Het recht op inzage kan afgewezen worden in bijzondere omstandigheden zoals beschreven in artikel 43 van de Wbp, bijvoorbeeld als dat nodig is in het belang van de voorkoming, opsporing en vervolging van strafbare feiten.
Het recht op informatie is terug te vinden in de openbaarmaking van deze regeling (artikel 13) en het informeren bij controles (artikel 6, leden 2 en 6).

Artikel 11 Sancties
In artikel 16 van de CAR/UWO zijn de disciplinaire straffen voor ambtenaren opgenomen. De op te leggen disciplinaire straf, welke varieert van een schriftelijke berisping tot ontslag, is afhankelijk van de ernst van de overtreding. Voor medewerkers die geen ambtenaar zijn, is de CAR/UWO niet van toepassing.
Voor deze medewerkers kunnen andere maatregelen worden getroffen, uiteenlopend van het geven van een waarschuwing tot het opzeggen van de contractueel aangegane verplichting, een en ander afhankelijk van de ernst van de overtreding.
Los van de mogelijke sancties kan in voorkomende gevallen overgegaan worden tot aangifte bij de politie of terugvordering van toegebrachte schade.

Artikel 10 Onvoorziene omstandigheden
Bij onvoorziene omstandigheden beslist het college van burgemeester en wethouders.

Artikel 11 Openbaarmaking, intrekking en inwerkingtreding
De regeling 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 gevolgen zijn bij overtreding van de regeling. Naast verstrekking op papier, kan naar de regeling worden verwezen tijdens het opstarten van het systeem of van het programma. Op die manier is verzekerd dat de medewerkers zich bewust zijn van de regeling.
De Regeling internet- en e-mailgebruik 2006 wordt ingetrokken zodra deze regeling inwerking is getreden.