Regeling ICT- en informatiegebruik 2012

Het college van burgemeester en wethouders van de gemeente Rotterdam,

gelezen het voorstel van de wethouder Financiën, Bestuur, Organisatie en Volksgezondheid van 17 april 2012; met kenmerk 925593;

gelet op artikel 125, artikel 125ter, van de Ambtenarenwet en artikel 160, eerste lid, onder c, van de Gemeentewet en het bepaalde in de Wet bescherming persoonsgegevens;

overwegende dat:
- de Centrale Ondernemingsraad heeft ingestemd met het ontwerpbesluit;
- het wenselijk is een regeling vast te stellen waarin regels voor het gebruikvan gemeentelijke ICT-middelen en gemeentelijke informatie worden gesteld en waarin eveneens regels zijn opgenomen voor het monitoren van dit gebruik;
- het wenselijk is informatiebeveiliging, gelet op het belang hiervan voor decontinuïteit en rechtmatigheid van gemeentelijke werkprocessen, te betrekken in de ontwikkelingen in de manier van werken en het benaderen van gemeentelijke informatie; **besluit vast te stellen:**

Regeling ICT- en informatiegebruik 2012

Artikel 1 Begripsbepalingen

In deze regeling en de daarop berustende bepalingen wordt verstaan onder:
a. cluster: een door de gemeente beheerd cluster;
b. concerndirecteur: degene die belast is met het dagelijks beheer en dedagelijkse leiding van een cluster, dan wel de deelgemeentesecretaris die belast is met de leiding van een deelgemeente;
c. medewerker: ambtenaar in de zin van het Ambtenarenreglement ofdegene die op arbeidsovereenkomst of anderszins betaalde of nietbetaalde werkzaamheden voor een dienst of een deelgemeente verricht;
d. ICT-middelen: alle huidige en toekomstige elektronische informatie-encommunicatie faciliteiten en ICT-apparatuur, door of namens de concerndirecteur aan medewerkers beschikbaar gesteld, alsmede de privé ICT-middelen indien en voor zover zij gebruikt worden op de werkplek en of voor de uitvoering van de door of namens de concerndirecteur opgedragen taken;
e. elektronische informatie- en communicatiefaciliteiten: sociale media, e-mail-, internet- en telefoonfaciliteiten;
f. ICT-apparatuur: elektronische informatie en communicatiemiddelen,inclusief alle bijbehorende hard- en software en bestanden;

g. functionaris informatiebeveiliging: door de concerndirecteur aangewezenaanspreekpunt voor informatiebeveiliging;
h. gemeentelijke informatie: alle gemeentelijke bestanden en informatiedoor of namens de concerndirecteur aan medewerkers beschikbaar gesteld, hieronder begrepen informatie van ketenpartners;
i. beveiligingsincident: gebeurtenis die een bedreiging vormt of kan vormenvoor de vertrouwelijkheid, integriteit of beschikbaarheid van gegevens;
j. beveiligingsclassificatie: overzicht van de risicoklassen van bestandsgegevens;
k. privé-bestand: bestand met een geheel of overwegend persoonlijkeinhoud;
l. privé ICT-middelen: ICT apparatuur in eigendom van medewerker zelf ofanderszins verkregen, zonder dat deze door of namens de concerndirecteur beschikbaar is gesteld;
m. persoonsgegeven: elk gegeven betreffende een geïdentificeerde ofidentificeerbare natuurlijke persoon in de zin van de Wet bescherming persoonsgegevens;
n. verwerken van persoonsgegevens: elke handeling of geheel vanhandelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, 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;
o. verkeersgegevens: gegevens die worden verwerkt voor het overbrengenvan communicatie over een elektronisch communicatienetwerk of voor de facturering ervan;
p. bestand: elk gestructureerd geheel van bedrijfs- of 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 betrekking heeft op verschillende personen of eenheden;
q. onrechtmatig gebruik dan wel misbruik van de ICT-middelen engemeentelijke informatie: een doen of nalaten in strijd met deze regeling of andere wet- en regelgeving.

Artikel 2 Reikwijdte

Deze regeling is voor alle medewerkers van toepassing op het gebruik van ICT-middelen en gemeentelijke informatie, ongeacht de plaats waar dit plaatsvindt en ongeacht de eigendom van de middelen waarmee de informatie wordt benaderd. Tevens is deze regeling van toepassing op de wijze waarop controle op dit gebruik plaatsvindt en op het verwerken van persoonsgegevens in dit kader.

Artikel 3 Gebruik van ICT-middelen en gemeentelijke informatie

1. Medewerkers gebruiken de ICT-middelen en gemeentelijke informatie primair en hoofdzakelijk voor het uitvoeren van de aan hen door de concerndirecteur opgedragen taken, in overeenstemming met wet- en

regelgeving en het doel waarvoor de middelen en informatie zijn verstrekt.
2. Het is medewerkers verboden om gemeentelijke ICT-middelen aan een ander ter beschikking te stellen. Gemeentelijke informatie mag slechts verstrekt worden aan daartoe geautoriseerde anderen.
3. De ICT-middelen en gemeentelijke informatie worden beschikbaar gesteld voor zakelijk gebruik. Privégebruik van gemeentelijke informatie en bestanden is niet toegestaan.
4. Incidenteel privégebruik van de overige ICT-middelen door medewerkers is toegestaan, mits dit gebruik in overeenstemming is met deze regeling en dit gebruik niet ten koste gaat van het uitvoeren van de aan de medewerkers door de concerndirecteur opgedragen taken. Gebruik van de ICT-middelen of gemeentelijke informatie voor commerciële doeleinden is niet toegestaan.
5. Het is medewerkers toegestaan gebruik te maken van privé ICTmiddelen voor de uitvoering van de hen opgedragen taken, mits de medewerkers zich hierbij houden aan de bepalingen van deze regeling en bevoegd zijn tot de voor de uitvoering van deze regeling noodzakelijke maatregelen. de concerndirecteur kan nadere regels stellen over het gebruik van privémiddelen.
6. Het is medewerkers niet toegestaan om de ICT-middelen of gemeentelijke informatie te gebruiken voor het opvragen, versturen, vastleggen of anderszins verwerken van pornografisch, erotisch, dan wel racistisch materiaal of informatie die naar algemeen maatschappelijke opvattingen als lasterlijk, beledigend, aanstootgevend of oneervol wordt beschouwd; mee te doen in chatsessies; online te gokken of te gamen; illegale software, films of muziek te downloaden; betaaldiensten af te nemen.
   Dit geldt niet indien de activiteiten nodig zijn voor de vervulling van de taak en hierover overleg heeft plaatsgevonden met de leidinggevende.
7. Het is medewerkers niet toegestaan met behulp van de ICT-middelen grote hoeveelheden software en bestanden te verzenden of op te vragen via het Rotterdamse bedrijfsnetwerk, waarvan de medewerker redelijkerwijs moet aannemen dat deze bestanden te omvangrijk zijn. Het is niet toegestaan een elektronisch bericht massaal te verzenden. Dit geldt niet indien de activiteiten nodig zijn voor de vervulling van de taak en hierover overleg heeft plaatsgevonden met de leidinggevende.
8. Medewerkers dienen bij het gebruik van de ICT-middelen en gemeentelijke informatie de nodige zorgvuldigheid te betrachten en de integriteit en goede naam van de gemeente te waarborgen.
9. Medewerkers dienen de gestelde beveiligingseisen ten aanzien van ICTmiddelen en gemeentelijke informatie in acht te nemen.
10. Medewerkers dienen schade aan, verlies of diefstal van ICT-middelen of gemeentelijke informatie onverwijld bij de leidinggevende te melden.

Artikel 4 Toegang tot en beveiliging van gemeentelijke informatie

1. De medewerker verschaft zich uitsluitend toegang tot die gegevenswaartoe hij geautoriseerd is.

2. Het is de medewerker verboden om anderen dan daartoe geautoriseerdemedewerkers toegang tot gemeentelijke informatie te verlenen.
3. De medewerker neemt passende technische en organisatorischemaatregelen om gemeentelijke informatie te beveiligen tegen verlies of tegen enige vorm van onrechtmatige gebruik.
   De medewerker houdt hierbij in ieder geval rekening met:
   a. de beveiligingsclassificatie van de informatie;
   b. de door de gemeente gestelde beveiligingsvoorschriften;
   c. aan de werkplek verbonden risico's;
   d. het risico door het benaderen van gemeentelijke informatie metandere dan door de gemeente verstrekte of goedgekeurde ICTapparatuur.
4. De medewerker dient geconstateerde of vermoede beveiligingslekken enbeveiligingsincidenten onverwijld te melden bij de functionaris informatiebeveiliging.
5. Ingeval van dringende redenen kan de concerndirecteur, of bij diensafwezigheid de functionaris informatiebeveiliging, dan wel de algemeen directeur van de Rotterdamse Service Organisatie besluiten tot het nemen van noodmaatregelen voor de informatiebeveiliging. Deze noodmaatregelen kunnen, voor zover dit noodzakelijk is, betrekking hebben op privé-middelen en privé-bestanden.
6. De medewerker is gerechtigd advies of ondersteuning van defunctionaris informatiebeveiliging te vragen.
7. De medewerker is verplicht advies of ondersteuning van deleidinggevende of de functionaris informatiebeveiliging te vragen indien de medewerker onvoldoende in staat is de beveiligingsvoorschriften uit te voeren of te beoordelen.
8. De beveiligingclassificatie en de beveiligingsvoorschriften als bedoeld inhet derde lid, zijn op te vragen bij de functionaris informatiebeveiliging.

Artikel 5 Controle

1. Controle door of in opdracht van de concerndirecteur op het gebruik vande ICT-middelen en gemeentelijke informatie vindt slechts plaats in het kader van de in artikel 7, eerste lid, 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 ICT-middelen en gemeentelijke informatie wordt beperkt tot de verkeersgegevens, die betrekking hebben op tijd, hoeveelheid, omvang en dergelijke.
   b. Controle ter voorkoming van onrechtmatig gebruik dan wel misbruikvan de ICT-middelen en gemeentelijke informatie 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. Voor zover de controle autorisatie of authenticatie betreft kan de controle autorisatiegegevens betreffen.
   c. Controle in het kader van het beheer van de toegang tot de systemenen 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 als regel plaats op het niveau van getotaliseerdegegevens die niet herleidbaar zijn tot individuele personen.
3. Indien een medewerker wordt verdacht van het overtreden van dezeregeling, kan gedurende een vastgestelde periode gerichte controle plaatsvinden.
4. Deze gerichte controle wordt slechts uitgevoerd nadat de medewerker isingelicht dat signalen hierover zijn ontvangen en om zijn reactie is gevraagd. De concerndirecteur 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.
5. Controle beperkt zich tot autorisatie- en verkeersgegevens van hetgebruik van de ICT-middelen of gemeentelijke informatie, tenzij sprake is van zwaarwegende redenen. Alleen bij zwaarwegende redenen kan er controle op de inhoud plaatsvinden. Privé-bestanden worden hierbij zoveel mogelijk ontzien.
6. Onrechtmatig gebruik dan wel misbruik van de ICT-middelen engemeentelijke informatie wordt zo veel mogelijk softwarematig onmogelijk gemaakt.
7. De medewerker die voor de uitvoering van de door de concerndirecteuropgedragen taken gebruik maakt van privé ICT-middelen is verplicht mee te werken aan eventuele controles volgens dit artikel. Hierbij worden de regels van dit artikel in acht genomen.
8. De in het eerste en tweede lid van dit artikel genoemde controles kunnentevens plaatsvinden door de algemeen directeur van de Rotterdamse Service Organisatie in het kader van het in artikel 7, lid 1,onder f, genoemde beheer van de ICT-middelen.
9. In het kader van kostenbeheersing van het gebruik van ICT-middelenverstrekt de algemeen directeur van de Rotterdamse Service Organisatie eens per kwartaal een overzicht van de per medewerker gemaakte kosten van het gebruik van ICT-middelen aan de voor die kosten verantwoordelijke dienst.
10. Indien geconstateerd wordt dat een medewerker zich niet houdt aan debepalingen van deze regeling, wordt de betrokken medewerker zo spoedig mogelijk hierop aangesproken door zijn leidinggevende.
11. Het gebruik van de ICT-middelen en gemeentelijke informatie door ledenvan de ondernemingsraden, Centrale Ondernemingsraad, Informeel Overleg en Georganiseerd Overleg, bedrijfsartsen en andere medewerkers met een vertrouwensfunctie, is in beginsel uitgesloten van controle. Dit geldt niet voor de controle op de veiligheid van het elektronische verkeer, voor de overzichten als genoemd in het achtste lid en voor informatie die geen verband houdt met genoemde functies of lidmaatschappen.

Artikel 6 Sancties

1. Medewerkers die ambtenaar zijn en deze regeling niet naleven, kunnendisciplinair worden bestraft als bedoeld in het Ambtenarenreglement.
2. Medewerkers, die geen ambtenaar zijn en deze regeling niet naleven,mogen, al dan niet tijdelijk, geen ICT-middelen en gemeentelijke informatie gebruiken, onverminderd de bevoegdheid van de concerndirecteur dan wel het college de contractuele relatie te beëindigen.

Artikel 7 De verwerking van persoonsgegevens van medewerkers

1. De verwerking van persoonsgegevens inzake het gebruik van ICTmiddelen en gemeentelijke informatie heeft de volgende doeleinden:
   a. het verkrijgen van inzicht in de aard en mate van het gebruik van de ICT-middelen en gemeentelijke informatie;
   b. het voorkomen van onrechtmatig gebruik dan wel misbruik van de ICT-middelen en gemeentelijke informatie;
   c. het beveiligen van het systeem en het netwerk;
   d. het beschermen van de privacy van de medewerkers op dewerkplek;
   e. het beschermen van de integriteit en goede naam van de gemeente;
   f. het beheer van de ICT-middelen en toegang tot de gemeentelijke informatie;
   g. kostenbeheersing van het gebruik van ICT-middelen.
2. Van medewerkers kunnen de navolgende persoonsgegevens wordenverwerkt inzake het gebruik van gemeentelijke informatie of ICTmiddelen:
   a. geautomatiseerd verkregen logging gegevens;
   b. naam en zakelijke persoonsgegevens bij incidentmeldingen;
   c. adresgegevens van de externe of mobiele werkplek;
   d. autorisatiegegevens;
   e. informatie over ter beschikking gestelde ICT-middelen engemeentelijke informatie;
   f. informatie over het gebruik van ICT-middelen en gemeentelijkeinformatie;
   g. kosten van het gebruik van ICT-middelen.
3. De concerndirecteur treft de nodige maatregelen opdat de verwerkingvan persoonsgegevens plaatsvindt conform de regels van de Wet bescherming persoonsgegevens. Dit betreft met name maatregelen: a. opdat de persoonsgegevens juist en nauwkeurig zijn;
   b. om de persoonsgegevens te beveiligen;
   c. voor het goede beheer van de persoonsgegevens.
4. De bewaartermijn van persoonsgegevens is zes maanden. Indien depersoonsgegevens het gebruik van de GBA betreffen, is deze termijn één jaar.
   Persoonsgegevens die ouder zijn worden verwijderd, tenzij er bijzondere redenen zijn om de gegevens langer te bewaren.
5. Indien gegevens ingevolge het vierde lid langer worden bewaard, wordtde medewerker hierover geïnformeerd vóór het ingaan van de verlenging van de bewaartermijn.

6. Indien de functionaris die belast is met het beheer van de bestandendelen niet kan verwijderen, wordt onder verwijderen verstaan het niet meer verstrekken van deze gegevens voor de in het eerste lid geformuleerde doeleinden.

Artikel 8 Rechten van de medewerker

1. De medewerker heeft het recht om een kopie van een overzicht teontvangen van de hem betreffende persoonsgegevens die worden verwerkt. De medewerker kan daartoe een schriftelijk verzoek indienen bij de concerndirecteur.
2. Indien de betreffende persoonsgegevens feitelijk onjuist, voor het doel ofde doeleinden van de verwerking onvolledig of niet ter zake dienend zijn, dan wel anderszins in strijd met een wettelijk voorschrift worden verwerkt, kan de medewerker de concerndirecteur schriftelijk verzoeken deze te verbeteren, aan te vullen, te verwijderen of af te schermen. Het verzoek bevat de aan te brengen wijzigingen.
3. De concerndirecteur bericht de medewerker binnen vier weken naontvangst van het in het tweede lid genoemde verzoek schriftelijk of, dan wel in hoeverre, hij daaraan voldoet. Een weigering is met redenen omkleed.
4. De concerndirecteur draagt er zorg voor dat een beslissing totverbetering, aanvulling, verwijdering of afscherming zo spoedig mogelijk wordt uitgevoerd.

Artikel 9 Onvoorziene omstandigheden

In gevallen waarin deze regeling niet voorziet of bij twijfel over de toepasselijkheid van deze regeling, beslist de concerndirecteur.

Artikel 10 Openbaarmaking

De concerndirecteur stelt de medewerkers die gebruik maken van de ICTmiddelen en gemeentelijke informatie op de hoogte van deze regeling.

Artikel 11 Intrekking oude regeling

De Regeling ICT-gebruik 2010 wordt ingetrokken.

Artikel 12 Inwerkingtreding

Deze regeling treedt in werking de dag na publicatie van het gemeenteblad.

Artikel 13 Citeertitel

Deze regeling wordt aangehaald als: Regeling ICT- en informatiegebruik 2012.

Aldus vastgesteld in de vergadering van 17 april 2012.

De secretaris, De burgemeester,

A.H.P. van Gils A. Aboutaleb

Dit gemeenteblad is uitgegeven op 18 april 2012 en ligt op werkdagen van 8.30 tot 16.00 uur ter inzage bij het Kenniscentrum Bestuursdienst Rotterdam (KBR), locatie Stadswinkel Centrum, Coolsingel 40 (zijde Doelwater, tegenover hoofdbureau politie)
(Zie ook: www.bds.rotterdam.nl – Gemeentebladen)

Toelichting regeling ICT- en informatiegebruik 2012

1. Algemeen

De onderhavige regeling ICT- en informatiegebruik vervangt de regeling ICTgebruik 2010 en breidt deze tegelijk uit.

De regeling ICT- en informatiegebruik regelt het gebruik door medewerkers van alle gemeentelijke ICT-middelen:

1. communicatiefaciliteiten (e-mail, Internet, telefoon);
2. ICT-apparatuur, inclusief software en bestanden; en
3. bestanden en informatie in alle denkbare vormen.

Deze elementen geven de ontwikkeling van de diverse regelingen weer: regeling e-mail en Internet. 2006 (1) regeling ICT-gebruik 2010 (1 en 2) regeling ICT- en informatiegebruik 2012 (1, 2 en 3)

1a. Wat is nieuw in deze regeling

- De regels zijn ook van toepassing op het gebruik van gemeentelijke informatie(bestanden).
- De beveiligingsregels zijn uitgebreid.
- De regels zijn ook van toepassing op het gebruik van privé-middelen in een zakelijke context, d.w.z.:
    - Als de medewerker werkzaam is in de kantooromgeving.
    - Op het moment dat de medewerker is ingelogd, of andere gemeentelijke ICT-middelen gebruikt.
    - Op het moment dat de werknemer gemeentelijke informatiegebruikt.

  De medewerker is dan werkzaam als werknemer van de gemeente Rotterdam. De gemeente kan voor deze activiteiten als werkgever aansprakelijk worden gesteld.

Aanleiding voor de nieuwe regels is de ontwikkeling van het nieuwe werken, met de daardoor toenemende risico's voor informatiebeveiliging en privacy. Ook bestaat de verwachting dat het gebruik van privé-middelen door medewerkers gaat toenemen.

1b. De hoofdlijnen van de regeling ICT- en informatiegebruik

- ***Wie, waar of hoe dan ook, een computer, telefoon of bestand van de gemeente gebruikt, moet zich houden aan de regels van de regeling ICT- en informatiegebruik.***

- De regeling stelt regels:

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

▪ De regeling richt zich vooral op ICT, maar vanzelfsprekend gelden de normen van zorgvuldigheid e.d. evenzeer voor papieren informatie en overige middelen die door de gemeente aan medewerkers ter beschikking worden gesteld.

- De voorwaarden waaraan het gebruik dient te voldoen, maken deel uit van het “goed werknemerschap”, zoals zorgvuldig omgaan met de gemeentelijke middelen en informatie, beschermen van de goede naam van de gemeente en voorkomen van aansprakelijkheid van de gemeente. De voorwaarden gelden daarom ook voor medewerkers die “als werknemer” gebruik maken van privé ICT-middelen.

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

- De privacybepalingen zijn vooral nodig vanwege de mogelijke bedreiging van de privacy bij een regeling als deze, waarbij persoonsgegevens worden verwerkt en controles kunnen plaatsvinden. Registratie van ICTgebruik, met daarmee controlemogelijkheden, vindt veelal automatisch en daardoor onmerkbaar plaats. Er moet duidelijk zijn wat wel en wat niet mag en welke rechten medewerkers hebben.

- Sancties worden vermeld omdat vooraf helder moet zijn dat het college dit onderwerp serieus neemt en, indien de omstandigheden daartoe aanleiding geven, ook streng zal optreden.

1c. De eigen verantwoordelijkheid van medewerkers.

Voor de medewerkers gaat het er niet alleen om wat mag en niet mag: van groot belang is ook de eigen verantwoordelijkheid van de medewerkers. Dit

was altijd al van belang, maar wordt nog eens extra benadrukt, nu door de grotere flexibiliteit voor de medewerkers onder het nieuwe werken het toezicht door de leidinggevende minder direct wordt uitgeoefend.

Dat er naast deze eigen verantwoordelijkheid toch nog regels worden gesteld heeft verschillende redenen:

1. Misbruik blijft altijd mogelijk en moet aangepakt kunnen worden. Daarvoor is vereist dat volstrekt duidelijk is wat niet is toegestaan.
2. Omdat het hier ICT-middelen en ICT-gebruik betreft kunnen controlesredelijk eenvoudig en vaak ongemerkt plaatsvinden. De privacywetgeving eist dan dat een regeling als deze is opgesteld.

Ook los van deze wat meer formele redenen, moet voor de medewerkers wel duidelijk zijn wat de grenzen zijn aan het gebruik van middelen en informatie. Deze grenzen worden vooral bepaald door de navolgende belangen:

- financiële belangen van de gemeente, (bijv. aansprakelijkheid, schade)
- goede naam van de gemeente (bijv. integriteit en gebruiksnormen)
- ongestoorde voortgang van de dienstverlening (bijv. beveiliging)
  - rechten van de burgers en werknemers (bijv. privacy)

Deze belangen vinden hun neerslag in de regels van deze regeling.

2. Gebruik van informatie, beveiliging onder het nieuwe werken.

Het nieuwe werken, samen te vatten als anywhere, anytime en any device, is in ontwikkeling. Vrije toegang tot informatie, het plaatsonafhankelijk werken en dergelijke principes trekken een zware wissel op informatiebeveiliging. Beveiligingsrisico's zijn er op verschillende niveaus:

- De locatie: openbare locaties (als internetcafés, hotels) vergroten het risico op meeluisteren, meekijken door kwaadwillenden. Openbare computers kunnen onveilig zijn.
- Het apparaat ('any device'): huisgenoten kunnen meekijken en mogelijk zelfs inloggen. Thuis PC's kunnen in een lokaal netwerk zijn opgenomen en benaderd worden vanaf een andere werkplek, mogelijk zelfs via een onbeveiligde draadloze verbinding. Bij verlies, afvoer van oude apparatuur kan data achterblijven en worden achterhaald.
- De verbinding: verbindingen kunnen worden afgeluisterd, data kan worden onderschept.
- Toegang tot informatie: informatie en bedrijfsapplicaties worden op afstand beschikbaar gesteld. Toegang met alleen naam en wachtwoord is eenvoudig te kraken.
- De mens: de mens is vaak de zwakste schakel: het apparaat wordt onbeheerd achtergelaten, een PC wordt soms niet goed beheerd en kan besmet zijn met malware of virussen. Datadragers (USB-sticks, Cd-roms) kunnen kwijtraken.

Ofschoon de risico's nieuw lijken zijn er geen principiële verschillen tussen: - toegang en gebruik van informatie binnen of buiten de kantooromgeving; - digitaal gebruik of gebruik van analoog/papieren dossier.

Het is in de kern dus de feitelijke context waarin organisatie en medewerkers weer nieuwe antwoorden moeten vinden. Hierbij is het zaak dat ieder zich

bewust is van de risico's en daarin ook nadrukkelijk de eigen verantwoordelijkheid neemt. Dit geldt voor de organisatie, die beveiligingsmaatregelen moet nemen en kaders moet stellen en voor medewerkers, die de maatregelen en kaders in acht moeten nemen en attent moeten blijven op de bestaande beveiligingsrisico's. Tegelijk blijven bestaande normen zoals eerder neergelegd in de regeling ICT-gebruik 2010 in deze nieuwe regeling normaal gelden.

De onderhavige regeling ICT- en Informatiegebruik 2012 beoogt beveiligingsbewustzijn en zorgvuldigheid bij het informatiegebruik te bewerkstelligen en het mogelijk te maken misbruik te sanctioneren. De noodzaak tot zorgvuldigheid is vooral afhankelijk van de mate van vertrouwelijkheid van de informatie, maar ook van belang zijn hierbij aspecten als beschikbaarheid en integriteit (juistheid) van de gegevens.

Deze factoren komen samen in de beveiligingsclassificatie, die een centrale rol in de beveiliging van gemeentelijke informatie speelt. Beschikbaarheid, integriteit en vertrouwelijkheid kennen elk 4 niveaus van beveiliging: geen, laag, midden en hoog. Het vaststellen van de beveiligingsclassificatie is een van de eisen die aan diensten worden gesteld bij het extern beschikbaar stellen van informatie. Degenen die vervolgens gebruik maken van die informatie moeten zich dan houden aan de beveiligingseisen, die aan de beveiligingsclassificatie zijn verbonden.

3. Artikelsgewijze toelichting

Artikel 1 Begripsbepalingen

De begrippen die in de Regeling ICT- en informatiegebruik 2012 (hierna: Regeling) voorkomen, worden in dit artikel gedefinieerd. Voor de omschrijving van verschillende begrippen is aangesloten bij de bewoordingen van de Wet bescherming persoonsgegevens (hierna: Wbp). De Wbp is van toepassing als er sprake is van verwerking van persoonsgegevens. Gegevens met betrekking tot het ICT- en informatiegebruik van medewerkers zijn in het algemeen te kwalificeren als persoonsgegevens.

De functionaris informatiebeveiliging heeft binnen een dienst of deelgemeente een centrale rol voor de informatiebeveiliging. Indien geen beveiligingsfunctionaris of vervangend aanspreekpunt is aangewezen, komt de leidinggevende daarvoor in de plaats. Met sociale media wordt gedoeld op fenomenen als hyves, facebook, twitter en yammer en eventueel toekomstige ontwikkelingen op dit gebied.

Artikel 2 Reikwijdte

De regeling is van toepassing op alle gebruik van ICT-middelen en gemeentelijke informatie: ongeacht de plaats, dus zowel binnen als buiten de kantooromgeving, en ongeacht de eigendom van de middelen waarmee de informatie wordt benaderd. De regeling is dus van toepassing op alle ICT- en informatiegebruik, zodra het gaat om gemeentelijke ICT-middelen, gemeentelijke informatie en/of de uitvoering van de functie. Een voorbeeld hiervan is het downloaden van illegale software. Dit is niet toegestaan onder de regeling, maar als dat privé met een privé-computer voor privédoeleinden wordt gedaan is dat de verantwoordelijkheid van de medewerker zelf. Het

gebruik daarna van deze software voor het werk is echter verboden zonder toestemming van de leidinggevende, ook omdat de gemeente hiervoor aansprakelijk kan worden gesteld.
In dit artikel wordt geregeld dat de regeling van toepassing is op alle medewerkers die werkzaam zijn bij de diensten en de deelgemeenten van de gemeente Rotterdam. De rechtsverhouding tussen hen en de werkgever is derhalve niet relevant. Zo hebben bijvoorbeeld ook uitzendkrachten, externe adviseurs en andere medewerkers die een tijdelijk contract met een dienst of een deelgemeente zijn aangegaan, zich te houden aan deze regeling. Zij moeten hierover dan vanzelfsprekend wel worden geïnformeerd.

Artikel 3 Gebruiksregels
De werkgever kan op basis van zijn gezagsbevoegdheid voorwaarden stellen aan het gebruik van ICT-middelen en informatie of bepaalde soorten gebruik verbieden.
Voor de hand ligt, dat de eerste voorwaarde betreft dat de gemeentelijke ICT-middelen en informatie moeten worden gebruikt voor het uitvoeren van de opgedragen taken. Daar zijn ze immers ook (uitsluitend) voor verstrekt.
Het verbod om de middelen aan een ander ter beschikking te stellen betreft zowel betaald als onbetaald ter beschikking stellen. Het is vanzelfsprekend wel toegestaan om de telefoon of dergelijke even te laten gebruiken door een collega.
Het derde lid geeft aan dat de middelen en informatie verstrekt zijn voor zakelijk gebruik. Dit geldt in het bijzonder voor gemeentelijke informatie, waarvan privégebruik - in het geheel - niet is toegestaan. Dit geldt voor alle gemeentelijke informatie (die niet openbaar is), waar je als medewerker toegang tot hebt. Incidenteel privégebruik van de overige ICT-middelen (apparatuur en communicatiefaciliteiten) is ingevolge het vierde lid beperkt toegestaan. Dit gebruik mag niet ten koste gaan van de dagelijkse werkzaamheden.
Uitgangspunt blijft het (100%) zakelijk gebruik. Dit geldt vooral op de werkplek en tijdens werktijd. Het is echter incidenteel wel eens noodzakelijk om op de werkplek of tijdens werktijd privézaken te regelen. Dit is daarom ook toegestaan.

Privégebruik van de privé-computer in privé-tijd valt buiten de regeling, maar ook voor het gebruik van de privé-computer op de werkplek geldt dat privégebruik slechts beperkt is toegestaan.

Lid 5 geeft aan dat medewerkers bij de uitvoering van hun functie gebruik mogen maken van privé ICT-middelen, maar zich dan wel moeten houden aan de regeling.
Logischerwijs gaat het hier vooral om het tegengaan van ongewenst gebruik, beveiliging en belasting van het netwerk en minder over het zorgvuldig omgaan met de apparatuur.
Het hoofd van dienst kan nadere regels stellen over het gebruik van privé ICT-middelen. Bijvoorbeeld over aan de middelen te stellen eisen of eventuele tegemoetkomingen.
Normaliter zal de werknemer eigenaar zijn van het privé-middel, maar dit behoeft niet altijd het geval te zijn. Daarom is een verdere voorwaarde, dat

de medewerker bevoegd moet zijn tot de voor de uitvoering noodzakelijke maatregelen als beveiligingsmaatregelen en meewerken aan controles.

Het zesde lid omschrijft het ongewenst gebruik. Dit is geen uitputtende opsomming.
In een enkel geval is denkbaar dat dergelijk gebruik functioneel is voor bijvoorbeeld beleidsvoorbereidend onderzoek. In dat geval is het noodzakelijk dit vooraf met de leidinggevende te bespreken. Dit geldt in het bijzonder voor clouddiensten (extern laten verwerken of opslaan van gegevens) en het gebruik van sociale media.

Waar het zesde lid vooral toeziet op de inhoud van de – ongewenste – informatie, ziet het zevende lid vooral toe op risico's en belasting van het netwerk. Met massaal verzenden wordt erop gedoeld dat het niet is toegestaan een elektronisch bericht aan alle of vrijwel alle medewerkers van de dienst tegelijkertijd te versturen.

De zorgvuldigheid en integriteit van de gemeente, zoals verwoord in lid 8 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 9 ziet toe op de beveiliging als onderdeel van de gebruiksnormen. Hier betreft dit vooral reeds genomen maatregelen, die gerespecteerd moeten worden.
Voorbeelden zijn het gebruik van encryptie, wachtwoorden of het gebruik van een beveiligde USB-stick.
De informatiebeveiligingsaspecten worden verder uitgewerkt in artikel 4.
De verplichting van het tiende lid om schade, verlies en diefstal meteen te melden zorgt ervoor dat zo snel mogelijk maatregelen genomen kunnen worden. De leidinggevende of functionaris informatiebeveiliging meldt dit vervolgens aan de beheerorganisatie (zoals de Servicedienst).

Artikel 4. Toegang tot en beveiliging van informatie.
Artikel 4, lid 1 en lid 2.
Toegang tot elektronische bestanden wordt veelal geregeld via "authenticatie en autorisatie", dat wil zeggen dat je rechten hebt op het benaderen van een bepaald bestand of informatie. Dit gaat meestal volgens het principe "need to know": je mag alleen zien wat je nodig hebt voor je functie. Doorgaans is hiervoor een technische voorziening (bijvoorbeeld via inlognaam), waardoor de computer alleen die bestanden opent waarvoor je bent geautoriseerd. In de analoge omgeving komt dit bijvoorbeeld neer op het mogen gebruiken van een sleutel voor een afgesloten ruimte waar bestanden staan.

Het eerste lid regelt dat je inderdaad alleen die gegevens mag benaderen, waarvan je weet of moet weten dat je daar toegang tot hebt. Fouten in autorisaties of beveiliging betekenen niet dat de informatie vrij is. Het tweede lid bepaalt vervolgens, dat je anderen ook geen gelegenheid mag geven om ongeautoriseerde toegang te verkrijgen.

Artikel 4, lid 3.
De medewerker is verplicht om passende maartregelen te treffen. Passend betekent voor dat moment in die situatie. Dus rekening houdend met eventueel veranderde omstandigheden die zwaardere beveiligingseisen stellen.
Hierin is ruimte gemaakt voor de eigen verantwoordelijkheid van de medewerker die, zo nodig met advies van de functionaris informatiebeveiliging, een beoordeling maakt. Wat passend is, is vooral afhankelijk van de risico's. De beveiligingsclassificatie is hiervoor de centrale maatstaf.

a. beveiligingsclassificatie

Voordat een bestand voor gebruik buiten de kantooromgeving beschikbaar wordt gesteld, moet de beveiligingsclassificatie van die informatie door de dienst zijn vastgesteld.
Niet altijd is er een door de dienst vastgestelde beveiligingsclassificatie. In dat geval is het aan de medewerker om te bepalen of de gegevens al dan niet vertrouwelijk of geheim zijn, of dat juist de eisen van beschikbaarheid of integriteit van de gegevens vragen om zware maatregelen voor informatiebeveiliging. De medewerker is meestal wel redelijk in staat dit in te schatten, omdat het bestand deel uitmaakt van zijn werk. Hierbij gaat het om de vragen:
- hoe vertrouwelijk zijn de gegevens;
- hoe erg is het als het bestand voor enige tijd niet beschikbaar is;
- hoe belangrijk is de juistheid van de gegevens.

Het belang wordt uitgedrukt in geen, laag, midden of hoog. De hoogste score bepaalt de beveiligingsclassificatie. Onderstaand schema kan hierbij behulpzaam zijn.
(zie ook handreiking beveiligingsclassificatie)

Classificatieniveau	**Beschikbaarheid**	**Integriteit**	**Vertrouwelijkheid**
"Geen"	Niet nodig	Niet zeker	Openbaar
"Laag"	Noodzakelijk	Beschermd	Bedrijfsvertrouwelijk
"Midden"	Belangrijk	Hoog	Vertrouwelijk
"Hoog"	Essentieel	Absoluut	Geheim

b. de gestelde beveiligingsvoorschriften.

Mogelijk zijn verschillende soorten beveiligingsvoorschriften:
- de algemene beveiligingsvoorschriften behorend bij de classificatie (bijvoorbeeld "hoog");
- algemene beveiligingsvoorschriften van een dienst (bijvoorbeeld bij de GGD);
- specifieke beveiligingsvoorschriften rond een bepaald bestand (bijvoorbeeld encryptie);
- beveiligingsvoorschriften rond een bepaald onderwerp (bijvoorbeeld bij thuiswerken) of bepaalde apparatuur (bijvoorbeeld een laptop). De beveiligingsvoorschriften worden per dienst verzameld bij de functionaris informatiebeveiliging of andere daartoe door de dienst aangewezen aanspreekpunt voor informatiebeveiliging (bijvoorbeeld bij de Servicedienst) en zijn daar opvraagbaar.

Uitgangspunt is dat de beveiligingsvoorschriften strikt worden nageleefd. Het beleid is daarop afgestemd en de organisatie moet hier ook vanuit kunnen gaan.
Toch kan een afwijking gerechtvaardigd zijn, bijvoorbeeld indien de genomen maatregelen verder gaan dan is voorgeschreven. Een dergelijke afwijking moet vooraf worden getoetst door de beveiligingsfunctionaris.

c. aan de werkplek verbonden risico's.

Het benaderen van een bestand vanuit een openbare locatie brengt heel andere risico's met zich mee dan wanneer dit vanuit de kantooromgeving plaatsvindt. Denk aan het meekijken door derden of aan verbindingen of apparatuur.

d. het risico door het benaderen van gemeentelijke informatie met andere dan door de gemeente verstrekte of goedgekeurde ICT-apparatuur.

Extra aandacht is vereist bij het gebruik van ICT-apparatuur (inclusief software), die niet door de gemeente is verstrekt of goedgekeurd. De medewerker mag de gemeentelijke informatie alleen benaderen indien de apparatuur die hij gebruikt, gelet op de beveiligingsclassificatie, voldoende betrouwbaar is.

Artikel 4, lid 4.
Het vierde lid introduceert een meldplicht voor alle soorten beveiligingsincidenten. Dit geldt ook voor vermoede fouten in beveiligingseisen of voorschriften. Feitelijk vraagt dit van alle medewerkers om alert te zijn op informatiebeveiliging. Dit is noodzakelijk om binnen een grote organisatie als de gemeente grip te houden op dit onderwerp.

Een andere reden voor de opgenomen meldplicht is dat er naar verwachting een wettelijke meldplicht voor beveiligingsincidenten zal ontstaan.
Melding vindt plaats bij de functionaris informatiebeveiliging. Voor zover het persoonsgegevens betreft, worden de meldingen opgenomen in het privacy jaarverslag.

Artikel 4, lid 5.
Het hoofd van dienst is bevoegd om noodmaatregelen te nemen ingeval van dringende redenen. Dit ziet toe op de situatie dat vertrouwelijke informatie of gegevens in verkeerde handen dreigen te vallen, doordat bijv. een mobiele telefoon of laptop is kwijtgeraakt of gestolen.
Dan bestaat bijv. de mogelijkheid alle informatie op afstand te wissen.
Dit geldt dan ook voor de privé-informatie die op het ICT-middel is opgeslagen.
Een dergelijke noodmaatregel kan ook worden toegepast op privé-middelen.
Het spreekt vanzelf dat voldoende aanleiding moet zijn voor het nemen van een dergelijke maatregel. Dit vergt een afweging van het hoofd van dienst. Indien deze niet beschikbaar is, is de functionaris informatiebeveiliging hiervoor aangewezen.
Ook kan de dringende reden voor noodmaatregelen zich voordoen bij de algemeen directeur van de Servicedienst, bijvoorbeeld in het kader van het

beheer van de ICT-middelen en toegang tot de gemeentelijke informatie. In dat geval is de algemeen directeur van de Servicedienst hiertoe bevoegd. Indien er tijd en gelegenheid is dit vooraf met het betreffende hoofd van dienst te overleggen, dient dit overleg plaats te vinden.
Na een dergelijk besluit kan dit worden getoetst met de vraag of het hoofd van dienst c.q. de functionaris danwel de algemeen directeur van de Servicedienst in redelijkheid tot dat besluit konden komen (zgn. marginale toetsing).

Artikel 4, leden 6, 7 en 8.
De functionaris voor de informatiebeveiliging wordt ingezet om de informatiebeveiliging binnen een dienst in goede banen te leiden en de medewerkers hierin te begeleiden.
Medewerkers zijn ingevolge het zesde lid altijd gerechtigd advies of ondersteuning te vragen van de functionaris voor de informatiebeveiliging. Om de functionaris voor de informatiebeveiliging niet al te veel te belasten wordt geadviseerd om eerst na te gaan of de gevraagde kennis niet al aanwezig is binnen de eigen afdeling.
Het zesde lid gaat hierin verder: de medewerkers zijn verplicht om hun leidinggevende of de functionaris voor de informatiebeveiliging in te schakelen indien zij niet voldoende in staat zijn om de beveiligingsvoorschriften uit te voeren.
Het meest voor de hand ligt hiervoor de leidinggevende te benaderen, maar soms kan het nodig zijn de functionaris voor de informatiebeveiliging in te schakelen.
Dit biedt de functionaris voor de informatiebeveiliging en/of de leidinggevende de mogelijkheid tot ondersteuning dan wel om andere maatregelen te nemen om de informatiebeveiliging te waarborgen. Onduidelijkheid kan daarmee nooit een reden zijn voor het verwaarlozen van informatiebeveiliging.
Het zevende sluit hierbij aan. De beveiligingsvoorschriften zijn verzameld, beschikbaar en daarmee voldoende kenbaar voor de medewerkers. Het spreekt voor zich dat de functionaris voor de informatiebeveiliging ervoor moet zorgen dat de informatie volledig en up to date is.

Artikel 5. Controles.

Artikel 5, eerste lid, onder a.
Voor het verkrijgen van inzicht in de mate van het gebruik van de ICTmiddelen en informatie, zal de controle beperkt kunnen blijven tot verkeersgegevens (tijd, hoeveelheid, omvang en dergelijke). Kennisneming van de inhoud of individuele gebruikers is dan niet noodzakelijk.

Artikel 5, eerste lid, onder 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 (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 werknemer. In beginsel zal de controle op naleving slechts steekproefsgewijs en geanonimiseerd mogen geschieden. Indien de

(steekproefsgewijze) controle de toegang tot informatie betreft, is noodzakelijk hierbij authenticatie en/of autorisatiegegevens te betrekken. Deze gegevens zijn niet geanonimiseerd.

Artikel 5, 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 5, tweede lid.
Het is in het algemeen niet noodzakelijk om het hoofd van dienst rapportages en gebruiksstatistieken van het ICT-gebruik van de medewerkers op persoonsniveau te verstrekken. De gegevens in de rapportages en statistieken zullen dus ontdaan moeten worden van hun identificerende kenmerken. Alleen als er concrete verdenkingen bestaan tegen een bepaalde medewerker, is rapportage op persoonsniveau noodzakelijk en dan ook toegestaan, volgens de regels van het derde en vierde lid.
Dit geldt niet voor de in het negende lid genoemde overzichten in het kader van kostenbeheersing, die betrekking hebben op de gemaakte telefoonkosten per medewerker.

Artikel 5, derde lid.
Gerichte controle op een persoon vindt slechts plaats indien een medewerker wordt verdacht van het overtreden van deze regeling en er sprake is van zwaarwegende belangen van de gemeente. Gerichte controle mag niet structureel zijn, maar is altijd tijdelijk.
Artikel 5, vierde lid.
Vindt gerichte controle plaats, dan dient de betrokken medewerker vooraf te worden geïnformeerd en om zijn reactie gevraagd. Deze informatieplicht kan worden opgeschort voor zover dit noodzakelijk 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 andereopenbare lichamen;
d) het toezicht op de naleving van wettelijke voorschriften die zijn gesteldten behoeve van de belangen, bedoeld onder b en c; of
e) de bescherming van de betrokkene of van de rechten en vrijheden vananderen (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 noodzakelijkheidsvereiste van artikel 43 Wbp dwingt tot een expliciete afweging ingeval niet vooraf wordt geïnformeerd. In dat geval moet altijd wel

alsnog achteraf worden geïnformeerd dat een onderzoek heeft plaatsgevonden (ook indien bij het onderzoek geen afwijkingen zijn geconstateerd).

Artikel 5, vijfde lid.
Controles zijn in beginsel beperkt tot verkeersgegevens. Dit zijn gegevens met betrekking tot datum, tijd hoeveelheid en omvang. Slechts bij *zwaarwegende* redenen wordt er op de inhoud van communicatie of bestanden gecontroleerd.

Artikel 5, zesde lid.
Onrechtmatig gebruik dan wel 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.
Content filtering wordt binnen de gemeente toegepast, maar is, vanwege de constante bewegingen en veranderingen in het aanbod, niet sluitend.

Artikel 5, zevende lid.
Controles kunnen ook betrekking hebben op privé ICT-middelen, die zakelijk worden gebruikt. De medewerker is verplicht mee te werken aan de controles. Bij deze controles moeten de controleregels van dit artikel in acht worden genomen, rekening houdend met de eigendomssituatie van de ICTmiddelen.
In het bijzonder dat:
- de doeleinden van de controles beperkingen stellen aan de omvang en wijze van controle (lid 1):
- Privé-bestanden hierbij zoveel mogelijk worden ontzien (lid 5).

Artikel 5, achtste lid.
Controles vinden als regel plaats in opdracht van het hoofd van de dienst waar de medewerker werkzaam is. In het kader van het beheer van de ICTmiddelen kan ook de algemeen directeur van de Servicedienst opdracht geven voor controle-activiteiten op de ICT-middelen waarover hij het beheer voert. Dit zal echter nooit de inhoud van communicatie of bestanden kunnen betreffen.

Artikel 5, negende lid.
Eens per kwartaal worden op basis van de facturen van de telefoonaanbieder overzichten gemaakt van de gemaakte kosten per telefoonnummer. Deze overzichten worden gespecificeerd naar medewerker verstrekt aan de betreffende dienst. Medewerkers met buitengewoon hoge telefoonkosten kunnen hierop worden aangesproken. Deze overzichten bevatten geen gespreksgegevens.

Artikel 5, lid 10.
Een bepaalde tijd voor de opbouw van het dossier is toegestaan indien de omstandigheden daartoe aanleiding geven.

Indien de medewerker op zijn handelen in strijd met de regeling wordt aangesproken, is het raadzaam dat hij gewaarschuwd wordt voor de (rechtspositionele) gevolgen bij continuering van dit gedrag.

Artikel 5, lid 11.
Op grond van artikel 17 van de Wet op de ondernemingsraden (WOR) hebben de leden van de OR ten behoeve van hun OR werkzaamheden 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. Het hoofd van dienst kan zijn gezagsbevoegdheid dus niet aanwenden om het ICT-gebruik van OR-leden in functie te controleren. Op communicatie van en aan OR-leden in functie zijn de algemene wettelijke regels omtrent vertrouwelijke communicatie van toepassing. Ook de inhoud van het overig ICT-gebruik is geprivilegieerd. Hiervan mag het hoofd van dienst in beginsel geen kennis nemen. Het betreft hier echter geen absoluut verbod. Er kan van worden afgeweken in bepaalde situaties van plichtsverzuim, waarbij men kan denken aan het lekken van geheime of vertrouwelijke stukken.
Voor wat betreft de toegang tot en het gebruik van de GBA kan, vanwege GBA regels, geen uitzondering gemaakt worden voor de hier genoemde vertrouwensfuncties. Ook voor de kostenoverzichten van het achtste lid, die volledig los staan van de inhoud van communicatie, wordt geen uitzondering gemaakt.

Artikel 6 Sancties.
In artikel 79 van het Ambtenarenreglement 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 het Ambtenarenreglement 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 en/of terugvordering van toegebrachte schade.
Artikel 7 De verwerking van persoonsgegevens van medewerkers.
Vanwege privacyvereisten is het noodzakelijk om de doelen van het verwerken van persoonsgegevens en het uitvoeren van controles vooraf vast te stellen.
In het eerste lid wordt aan deze eisen voldaan.
Deze doeleinden moeten wel een wettelijke grondslag hebben (artikel 8 Wbp). In deze 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: - de aard, omvang en vorm van de verwerking en de controlemaatregelen dienen in een redelijke verhouding tot de genoemde doelen te staan; - de verwerking van persoonsgegevens en de controles mogen niet méér

inbreuk maken op de belangen van de medewerker dan strikt noodzakelijk is.

Artikel 7, tweede lid.
Het tweede lid geeft aan welke informatie van medewerkers wordt verwerkt in relatie tot het gebruik van ICT-middelen en informatie.
Logging gegevens geven informatie over “het bezoek” aan een bestand: welke gegevens zijn bekeken of opgevraagd etc. Logging is vaak een maatregel die nodig is in het kader van informatiebeveiliging of privacybescherming (van de burger).
Voor wat betreft de informatie over het gebruik van ICT-middelen verdient vooral het gebruik van communicatiefaciliteiten aandacht. Denk bijvoorbeeld aan alle bezochte internetadressen die worden vastgelegd of een telefoonregistratie die alle telefoonnummers bevat. Dit betreft veelal geautomatiseerd verwerkte gegevens die in eerste aanleg alleen verkeersgegevens betreffen (dus welke IP-adressen van computers of telefoonnummers). Koppeling van deze verkeersgegevens aan een persoon is echter een mogelijkheid, bijvoorbeeld in het kader van gerichte controle.

De gemeente is vanzelfsprekend gehouden aan de uitvoering van de Wet bescherming persoonsgegevens. Het college van burgemeester en wethouders is de “verantwoordelijke” in de zin van de Wbp.
Het derde lid geeft aan dat het hoofd van dienst de nodige maatregelen moet treffen.

Artikel 7, lid 3.
Met de “nodige” maatregelen wordt uitgedrukt 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 ommeer aandacht);
- de stand van de techniek;
- de kosten/benodigde inspanning van de maatregelen.

Lid 3 onder 3 betreft het beheer van de persoonsgegevens.
Eén of meer functionarissen (bijvoorbeeld beheerders) zijn met het beheer van informatiesystemen belast. Deze functionarissen hebben uit hoofde van hun functie toegang tot afgeschermde gegevens in het computernetwerk. Deze functie dient met de nodige waarborgen te worden omgeven. De functionaris 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. Deze functionaris is uiteraard in beginsel niet bevoegd tot het lezen van documenten of e-mail of het meekijken met het internetgebruik van de medewerkers. De functionaris dient tegenover het management een zekere onafhankelijkheid te hebben. Er moet dus binnen de dienst een heldere procedure zijn over wie in welke gevallen de genoemde functionaris opdracht kan geven om bepaalde zaken op het netwerk nader te controleren of daarover informatie te verschaffen. Artikel 5 is hiervoor het kader.

Artikel 7, lid 4.
Het is in het algemeen niet nodig om de persoonsgegevens lang te bewaren. De standaardtermijn is zes maanden. Waar het de GBA betreft geldt de termijn van 1 jaar.
In het geval van een zwaarwegend vermoeden van onrechtmatig gebruik dan wel misbruik van ICT-middelen en informatie, worden de gegevens 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.

Artikel 7, lid 5.
Indien de standaard bewaartermijn wordt verlengd volgens het vierde lid, moet de medewerker hierover vooraf worden geïnformeerd.
Concreet betekent dit dat de 6 maanden respectievelijk 1 jaar bewaartermijn niet overschreden kan worden zonder dat de medewerker hierover is geïnformeerd.

Artikel 7, lid 6.
Bepaalde gegevens kunnen soms om technische redenen niet worden verwijderd. Van het e-mailsysteem worden bijvoorbeeld back-ups gemaakt die in geval van nood teruggezet kunnen worden. Deze back-ups kunnen niet zonder meer gewist worden. Het is ook niet mogelijk om binnen een dergelijke back-up een individueel e-mailbericht te verwijderen. De bedoelde gegevens mogen in deze gevallen niet meer worden verstrekt (verwerkt).

Artikel 8 Rechten van de medewerker.
In dit artikel worden de rechten van de medewerkers bij het verwerken van persoonsgegevens behandeld.
Het eerste lid betreft het recht op inzage. Dit recht is geregeld in artikel 35 Wbp.
Het verzoek tot aanvullen, verbeteren, verwijderen of afschermen van de gegevens kan slechts plaatsvinden indien daarvoor een feitelijke reden is, als omschreven in het tweede lid. Dit is vastgelegd in artikel 36 Wbp. De in het derde lid genoemde motivering is nodig omdat een weigering een besluit in de zin van de Awb betreft.
Het recht op inzage kan buiten toepassing gelaten worden in bijzondere omstandigheden als vastgelegd in artikel 43 Wbp, bijvoorbeeld indien 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 10) en het informeren in het kader van controles (artikel 5, leden 4 en 10).

Artikel 9 Onvoorziene omstandigheden.
Bij onvoorziene omstandigheden beslist het betreffende hoofd van dienst namens het college van burgemeester en wethouders.

Artikelen 10, 11 en 12 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 ICT-gebruik 2010 wordt ingetrokken op het zelfde moment dat onderhavige regeling in werking treedt.