Nota voor Burgemeester en Wethouders

Team: Advies, Support en Kennis
Onderwerp:
vaststellen Privacyreglement email- en internetgebruik DOWR

Notagegevens		
Bestuursorgaan	:	B-en-W 19-04-2022
Notanummer	:	2022-316
Datum	:	19-04-2022
Programma	:	11-Bedrijfsvoering
Portefeuillehouder	:	Wethouder Verhaar,
Bijlage(n)	:	2022 Brief Instemmen OR Reglement e-mail en internetgebruik 2021.pdf,Reglement e-mail- en internetgebruik 2021 definitief.docx

Parafering

29-03-2022: Wethouder
05-04-2022: Programmamanager

Agendering

* 14-04-2022: adjunct-secretaris en teammanager Concernstaf
* 11-04-2022: Gemeentesecretaris/algemeen directeur

Definitieve akkoord

20-04-2022

B & W d.d.: 19-04-2022

Besluit

1. het "Privacyreglement email- en internetgebruik DOWR" vast te stellen.

De nota en het besluit openbaar te maken.

Inleiding

Het huidige reglement is verouderd. Het nieuwe reglement is aangepast conform Algemene Verordening Gegevensbescherming en de Wet Normalisering Rechtspositie Ambtenaren (AVG en Wnra) , is aangepast aan relevante jurisprudentie én er is in het voortraject een risicoanalyse (een DPIA) uitgevoerd op het proces ‘logging & monitoring’.

Beoogd maatschappelijk resultaat

Een actueel privacyreglement opnemen in het personeelshandboek DOWR. Het Privacyreglement geeft de wijze aan waarop in de DOWR-gemeenten wordt omgegaan met elektronische communicatiemiddelen en omvat regels ten aanzien van verantwoord gebruik hiervan en regels over de wijze waarop controle hiervan plaatsvindt.

Het reglement is van toepassing voor zowel de medewerkers in dienst van de DOWR-gemeenten, inhuur-medewerkers, als ook voor de collegeleden (de politieke ambtsdragers).

Dit reglement is ook bedoeld om medewerkers en collegeleden te informeren over de verwerking van hun persoonsgegevens die kan plaatsvinden bij het gebruik van

internet- en e-mailfaciliteiten van de gemeente.

Kader
De AVG , Burgerlijk Wetboek en de CAO Gemeenten .

Betrokken partijen en participatie
Er heeft afstemming plaatsgevonden tussen de drie HR functionarissen van de DOWR-gemeenten en met de Privacy Officer en de Information Security Officer (ISO). Ook in de andere twee DOWR-gemeenten is/wordt een vergelijkbaar voorstel in procedure gebracht.

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. Vooruitlopend op de aanpassing van dit privacyreglement heeft er een risico analyse plaats gevonden. De OR-en hebben daar recent kennis van genomen en hebben hier geen opmerkingen over gemaakt.

De OR Deventer heeft aangegeven het belangrijk te vinden dat medewerkers goed worden geïnformeerd over de verwerking van (hun) persoonsgegevens. Zodat ze zich er van bewust zijn dat gegevens worden verzameld, welke dat zijn en waarom dat wordt gedaan. De OR heeft daarbij geadviseerd de actualisatie van het reglement breed te communiceren en om alle DOWR-medewerkers nog eens goed (en op begrijpelijke wijze) te informeren over de inhoud van het reglement en de verwerking van hun persoonsgegevens. Aan dit advies wordt invulling gegeven na vaststelling van het reglement. Het advies van de OR treft u als bijlage bij deze nota aan.

Argumenten voor en tegen
Binnen de gemeente Deventer, Olst-Wijhe en Raalte 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 DOWR-gemeenten dan ook zaak daarover een duidelijk beleid te voeren. Omdat het huidige reglement is verouderd, is dit nu geactualiseerd. Er heeft een vertaling plaats gevonden van de AVG in het nieuwe DOWR reglement. Beschreven is in het nieuwe reglement wat is toegestaan en wat verboden is, op welke manier controle gebeurt én wat de consequenties kunnen zijn bij overtreding van het reglement?

Financiële consequenties en dekking
Niet van toepassing

Openbaarmaking en communicatie
Zodra het reglement is vastgesteld door de drie gemeenten zal een gezamenlijk communicatiebericht worden gemaakt waarin de kern van het reglement gecommuniceerd zal worden via Sharepoint.

Na vaststelling wordt het nieuwe reglement opgenomen in het personeelshandboek DOWR, waardoor het voor alle betrokkenen is te raadplegen.

Aanpak en uitvoering
zie bij openbaarmaking

DOWR Reglement e-mail- en internetgebruik 2021

Artikel 1 Definities
In dit reglement e-mail en internetgebruik (“Reglement") wordt verstaan onder:

1. AVG: Algemene Verordening Gegevensbescherming;
2. Gemeente: de gemeente Deventer, Olst-Wijhe of Raalte;
3. AP: de Autoriteit Persoonsgegevens;
4. Politieke ambtsdrager: een lid van het college;
5. Werknemer: degene die aan te merken is als:
   a. persoon met een arbeidsovereenkomst met de gemeente;
   b. persoon die (betaalde of niet-betaalde) werkzaamheden voor de gemeente verricht, anders dan op basis van een arbeidsovereenkomst;
6. E-mailfaciliteiten: de door of namens de gemeente aan werknemers en politieke ambtsdragers ter beschikking gestelde e-mail faciliteiten;
7. Internetfaciliteiten: de door of namens de gemeente aan werknemers 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 van gemeente Deventer, Olst-Wijhe of Raalte, 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 Reglement of met wet- en regelgeving of een inbreuk op een recht.

Artikel 2 Reikwijdte
Dit Reglement is van toepassing op het gebruik door werknemers en politieke ambtsdragers van elektronische communicatiemiddelen, inclusief de controle die daarop plaatsvindt door de verwerkingsverantwoordelijke. Dit Reglement bevat regels ten aanzien van verantwoord gebruik van elektronische communicatiemiddelen en regels over de wijze waarop controle hiervan plaatsvindt.

Artikel 3 (Persoons)gegevens
Bij het gebruik van elektronische communicatiemiddelen kan de verwerkingsverantwoordelijke de navolgende gegevens verwerken:

- gegevens ten behoeve van identificatie van en communicatie met de gebruikers binnen het netwerk;
- gegevens met betrekking tot bevoegdheden van de gebruiker en de netwerkbeheerder met het oog op de aangeboden faciliteiten en diensten van het netwerk;
- gegevens met betrekking tot de verrichtingen van de gebruikers en de netwerkbeheerder;
- gegevens met betrekking tot elektronische berichten afkomstig van of bestemd voor de gebruikers.

Meer specifiek (maar niet uitsluitend) kan de verwerkingsverantwoordelijke in dit verband het IP-adres, de accountnaam en het e-mailadres van de gebruiker verwerken.

Artikel 4 Doeleinden
De verwerking van persoonsgegevens door de verwerkingsverantwoordelijke met betrekking tot het gebruik van de elektronische communicatiemiddelen geschiedt slechts voor de volgende doeleinden:

1. capaciteitsbeheer;
2. het voorkomen en/of beëindigen van onrechtmatig gebruik dan wel misbruik van de elektronische communicatiemiddelen;
3. systeem- en netwerkbeveiliging;
4. bewijs en archivering;
5. continuïteit van de bedrijfsvoering en de dienstverlening;

6. het kunnen voldoen aan wettelijke verplichtingen in het kader van de AVG.

Artikel 5 Grondslagen

De volgende grondslagen voor de verwerking van persoonsgegevens zijn hier van toepassing:

1. Doel 6: de verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust (art. 6 lid 1 sub c AVG).
2. Doel 1-5: de verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke (art. 6 lid 1 sub f AVG).

Artikel 6 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. Deze beheerders krijgen passende (bewustwordings)trainingen ten aanzien van de omgang met persoonsgegevens.
4. Langdurige ziekte, ontslag, uitdiensttreding en noodsituaties (zoals bedoeld onder lid 5) kunnen met het oog op het bedrijfsbelang reden zijn om de teammanager en/of de arbeidsjurist toegang tot de mailbox of bestanden van de desbetreffende werknemer te geven.
5. In bijzondere situaties (bijvoorbeeld plichtsverzuim, ongewenst gedrag, arbeidsconflict, ernstig verstoorde verhoudingen) kan de toegang tot de mailbox of bestanden worden geblokkeerd.
6. Indien sprake is van lid 4 en/of lid 5 geeft de Algemeen Directeur van de betreffende gemeente hiervoor de opdracht.
7. Indien sprake is van lid 4 worden bestanden of e-mails die privé zijn zo veel als mogelijk ontzien.
8. Werknemers worden achteraf geïnformeerd over de uitkomst van een gericht onderzoek. Ook als is gebleken dat er geen sprake was van het overtreden van het Reglement.
9. Om te kunnen voldoen aan verzoeken in het kader van artikel 15 t/m 22 AVG (rechten van betrokkenen) kan de verwerkingsverantwoordelijke een geautomatiseerde zoekfunctionaliteit binnen gemeentelijke informatiesystemen toepassen. Met deze functionaliteit kan op basis van een specifieke zoekterm gezocht worden naar de locatie waar de persoonsgegevens van een verzoeker zich bevinden. Bij het toepassen van de functionaliteit krijgt de daartoe bevoegde medewerker (de information security officer, in aanwezigheid van de privacy officer) geen toegang tot de inhoud van e-mails of documenten. Deze krijgt alleen te zien op welke digitale locaties de gegevens van verzoeker zich bevinden en in welke hoeveelheden.

Artikel 7 Gebruik elektronische communicatiemiddelen

1. Werknemers 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 privégebruik van de elektronische communicatiemiddelen door werknemers en politieke ambtsdragers is toegestaan mits dit gebruik in overeenstemming is met dit Reglement 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 werknemers en politieke ambtsdragers niet toegestaan met behulp van e-mailfaciliteiten kettingbrieven te versturen of pornografisch materiaal te versturen of op te vragen, dan wel aanstootgevende, dreigende, lasterlijke, seksueel intimiderende, onzedelijke, racistische of discriminerende opmerkingen te maken. Evenmin is het werknemers en politieke ambtsdragers toegestaan met behulp van de e-mailfaciliteiten 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 werknemers en politieke ambtsdragers niet toegestaan met behulp van elektronische communicatiemiddelen 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. Ook is het niet toegestaan de elektronische communicatiemiddelen te gebruiken om mee te doen in chat-sessies (behoudens voor zakelijk gebruik), 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. Werknemers 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 dit nodig is voor hun taken en zij hiervoor, uit hoofde van hun onderzoeks- en controletaken, ook specifiek toestemming van de teammanager, hebben.
5. Indien werknemers en politieke ambtsdragers via de internetfaciliteiten gebruik maken van webe-mailtoepassingen (zoals hotmail, gmail, yahoo, outlook, et cetera), dan zijn de bepalingen van artikel 7, derde lid, van overeenkomstige toepassing.
6. Werknemers 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.

Artikel 8 Controle

1. Controle door de verwerkingsverantwoordelijke op het gebruik van de elektronische communicatiemiddelen vindt slechts plaats in het kader van de in artikel 4 genoemde doeleinden. Deze doeleinden stellen beperkingen aan de omvang en wijze van controle.
2. Controle in het kader van systeem- en netwerkbeveiliging vindt op geautomatiseerde wijze plaats.
3. Onrechtmatig gebruik dan wel misbruik van de elektronische communicatiemiddelen wordt zo veel mogelijk softwarematig onmogelijk gemaakt.
4. Een gerichte controle op onrechtmatig gebruik dan wel misbruik van de elektronische communicatiemiddelen vindt alleen plaats in geval van een redelijk vermoeden en na goedkeuring van de Algemeen Directeur van de betreffende gemeente. De gerichte controle heeft tot doel om vast te stellen of daadwerkelijk sprake is (geweest) van onrechtmatig gebruik dan wel misbruik van elektronische communicatiemiddelen. Bij dit onderzoek wordt rekening gehouden met het recht op vertrouwelijke communicatie van de betreffende werknemer. De Algemeen Directeur informeert de Ondernemingsraad zonder onredelijke vertraging over het inzetten van een gerichte controle. De Algemeen Directeur verstrekt daarbij geen persoonsgegevens aan de Ondernemingsraad en waar passend vindt verstrekking plaats onder oplegging van vertrouwelijkheid.
5. Indien geconstateerd wordt dat een werknemer dit Reglement overtreedt, dan wordt de betrokken werknemer zo spoedig mogelijk hierop aangesproken door de betreffende leidinggevende.
6. Het gebruik van de elektronische communicatiemiddelen door bijvoorbeeld OR-leden, LO-leden, mediators, bedrijfsartsen, andere werknemers met een vertrouwensfunctie en politieke ambtsdragers zijn in beginsel uitgesloten van controle. Dit geldt niet voor de controle ten behoeve van systeem- en netwerkbeveiliging.
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 9 Bewaartermijn

Persoonsgegevens die verwerkt worden inzake het gebruik van elektronische communicatiemiddelen worden verwijderd uiterlijk 6 maanden nadat zij zijn verkregen, tenzij de persoonsgegevens langer bewaard moeten worden om te kunnen voldoen aan een wettelijke bewaarplicht of de verwerkingsverantwoordelijke een gerechtvaardigd belang heeft bij het langer bewaren van de gegevens, zoals in het geval de gegevens nodig zijn ter onderbouwing van een rechtsvordering.

Indien en voor zover de persoonsgegevens zijn opgeslagen op back-ups worden deze (voor zover niet periodiek overschreven) maximaal 5 jaar bewaard.

Artikel 10 Rechten van de werknemer en politieke ambtsdrager

1. Aan de werknemer en de politieke ambtsdrager die daarom aan verwerkingsverantwoordelijke verzoekt, wordt een overzicht verschaft van de hem betreffende persoonsgegevens die worden verwerkt.
2. De werknemer 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. Daarnaast heeft de werknemer en de politieke ambtsdrager te allen tijde het recht om bezwaar te maken tegen een verwerking van persoonsgegevens.
3. De verwerkingsverantwoordelijke draagt er zorg voor dat een beslissing tot verbetering, aanvulling, verwijdering, afscherming of op bezwaar zo spoedig mogelijk – en in ieder geval binnen de daarvoor geldende wettelijke termijnen – wordt uitgevoerd.
4. De werknemer en de politieke ambtsdrager kunnen ten slotte een klacht indienen bij de Autoriteit Persoonsgegevens over de verwerking van hun persoonsgegevens. De werknemer en de politieke ambtsdrager zullen eerst van deze mogelijkheid gebruikmaken nadat een gesprek heeft plaatsgevonden met de Algemeen Directeur respectievelijk de burgemeester en dit gesprek vervolgens niet tot een bevredigende oplossing heeft geleid.

Artikel 11 Sancties

1. Overtreding van dit Reglement kan voor werknemers in dienst van de gemeente resulteren in disciplinaire maatregelen of in arbeidsrechtelijke consequenties met als meest vergaande maatregel ontslag op staande voet als sprake is van een dringende reden.
2. Overtreding van dit Reglement 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 tot kantoren, werkplaatsen of andere arbeidsterreinen;
   c. het ontbinden of opzeggen van de overeenkomst;
   d. verbod om nog langer werkzaamheden voor de gemeente te verrichten.
3. Overtreding van dit Reglement kan voor politieke ambtsdragers eveneens resulteren in sancties.
4. Bij strafbare feiten kan door of vanwege de gemeente aangifte worden gedaan.
5. De sancties genoemd onder lid 1 t/m 4 mogen niet eerder worden opgelegd dan nadat een zorgvuldig onderzoek naar de feiten is uitgevoerd en hoor en wederhoor heeft plaatsgevonden.

Artikel 12 Onvoorziene omstandigheden

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

Artikel 13 Openbaarmaking, inwerkingtreding en evaluatie

1. Dit Reglement wordt kenbaar gemaakt aan alle werknemers en politieke ambtsdragers die, direct of indirect, de beschikking krijgen over elektronische communicatiemiddelen en zal voor hen steeds raadpleegbaar zijn op een centrale digitale locatie. Bij het uitreiken van telefoons, laptops, tablets of andere devices aan nieuwe werknemers of politieke ambtsdragers zal dit Reglement voorts aan hen ter beschikking worden gesteld dan wel zal daarnaar uitdrukkelijk worden verwezen.
2. Dit Reglement is ter instemming voorgelegd aan de Ondernemingsraad en is door de Ondernemingsraad op […] goedgekeurd.
3. Dit Reglement treedt in werking op de dag na bekendmaking, onder gelijktijdige intrekking van het Privacyreglement e-mail- en internetgebruik, vastgesteld door burgemeester en wethouders op …… en in werking getreden met ingang van ……...
4. Dit Reglement wordt vierjaarlijks geëvalueerd door de verwerkingsverantwoordelijke en de Ondernemingsraad.

Toelichting

Algemeen
Binnen de gemeente Deventer, Olst-Wijhe en Raalte 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 DOWR-gemeenten dan ook zaak daarover een duidelijk beleid te voeren. Elektronische controle van computergebruik raakt echter ook 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 Reglement 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 Reglement voorkomen worden hier gedefinieerd. Voor de omschrijving van begrippen is zoveel 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 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 werknemer of politieke ambtsdrager. Dit noemen we ‘logging’. 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 werknemer de regels in het Reglement 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 Reglement is van toepassing op het gebruik van de elektronische communicatiemiddelen door werknemers en politieke ambtsdragers, inclusief de controle daarop. Het Reglement geldt voor alle werknemers van de gemeente: ambtenaren en personen die (betaald of niet-betaald) werkzaamheden voor de gemeente verrichten, anders dan op basis van een arbeidsovereenkomst. Daarnaast geldt het Reglement ook voor politieke ambtsdragers (zijnde collegeleden).

Telewerken
Indien de werknemer of politieke ambtsdrager vanuit zijn eigen huis inlogt op het computersysteem van het werk (telewerken), dan is dit Reglement van overeenkomstige toepassing. De computer van de werknemer of politieke ambtsdrager thuis maakt dan immers logisch gezien deel uit van het computernetwerk van de gemeente. In het geval van de werknemer geldt aanvullend dat hij/zij zich bevindt in een situatie waarin ook de gezagsbevoegdheid van de werkgever geldt.

Gastennetwerk
Indien een werknemer of politiek ambtsdrager gebruik maakt van een door de gemeente aangeboden gastennetwerk dan is het Reglement ook van toepassing.

Artikel 3 (Persoons)gegevens
Dit artikel geeft aan welke (persoons)gegevens de verwerkingsverantwoordelijke kan verwerken in het kader van controle op gebruik van de elektronische communicatiemiddelen.

Artikel 4 Doeleinden

Dit artikel geeft aan voor welke doeleinden de verwerkingsverantwoordelijke persoonsgegevens in het kader van controle op gebruik van de elektronische communicatiemiddelen mag gebruiken. De AVG bepaalt dat persoonsgegevens slechts voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden verwerkt mogen worden (artikel 5, lid 1, sub b AVG). Deze doelomschrijving moet nauwkeurig en zo volledig mogelijk zijn. Controle via volgsystemen is dus alleen toegestaan indien het doel van de controle vooraf is bepaald. In het Reglement zijn zes doeleinden geformuleerd. Concreet betekent dit dat logging alleen mag worden vastgelegd en gebruikt voor de in artikel 4 geformuleerde doeleinden. Het gebruiken van logging voor andere doeleinden is onrechtmatig.

Artikel 5 Grondslagen
Wettelijke verplichting (art. 6 lid 1 sub c AVG):
Deze grondslag is van toepassing op doel nummer 6 (zie de doeleinden genoemd in artikel 4). De verwerkingsverantwoordelijke moet kunnen voldoen aan verzoeken op grond van artikel 15 t/m 22 AVG. Hierbij kan het bijvoorbeeld in geval van een inzageverzoek nodig zijn om in logging te kunnen terugvinden welke accounts toegang hebben gehad tot bepaalde persoonsgegevens.

Gerechtvaardigd belang (art. 6 lid 1 sub f AVG):
Wat betreft de overige doelen genoemd in artikel 4 is de grondslag gerechtvaardigd belang van toepassing. Het gaat hier om de gerechtvaardigde belangen van de verwerkingsverantwoordelijke.

Artikel 6 Verantwoordelijkheden en beheer
Eerste lid
Op de verwerkingsverantwoordelijke wordt geen absolute verplichting gelegd. Een garantie voor de juistheid van gegevens kan van de verwerkingsverantwoordelijke 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.

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.
De verwerkingsverantwoordelijken hebben hiertoe onder verantwoordelijkheid van de proceseigenaar (manager DOWR-i) een data protection impact assessment (DPIA) uitgevoerd.

Derde lid
Een of meer beheerders zijn met het beheer van de bestanden belast. De netwerkbeheerder heeft uit hoofde van zijn functie toegang tot alle gegevens in het computernetwerk. De functie van netwerkbeheerder dient met de nodige waarborgen te worden omgeven. De netwerkbeheerder 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 netwerkbeheerder is uiteraard niet bevoegd tot het lezen van documenten of e-mail of het meekijken met het internetgebruik van de werknemers of politieke ambtsdragers zonder dat daar een bijzondere aanleiding voor is.

Vierde en vijfde en zesde lid
Het is ingeval van uitdiensttreding, langdurige ziekte van een werknemer 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 mails of bestanden niet verloren gaan. Tevens kan dit van belang zijn in het kader van de opvolging van de ex-werknemer. In bovenstaande gevallen wordt rekening gehouden met de privacybelangen van de (ex)-werknemer en de geldende normen omtrent kennisneming van privé-mail en bestanden.

Zevende lid
De verwerkingsverantwoordelijke dient het recht op privacy van een (ex)-werknemer of (ex)-politieke ambtsdrager te respecteren. Het lezen van privé-mail van een (ex)-werknemer of (ex)-politieke ambtsdrager is, behoudens bijzondere omstandigheden, niet toegestaan. Bij uitdiensttreding c.q. ontslag is de werknemer 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.

Negende lid
Personen waarvan de gegevens door een verwerkingsverantwoordelijke worden verwerkt hebben verschillende rechten om controle te houden op deze verwerking. Deze rechten staan genoemd in artikel 15 t/m 22 van de AVG. Zo kan een inwoner bijvoorbeeld op grond van artikel 15 AVG om inzage vragen in al zijn persoonsgegevens. De verwerkingsverantwoordelijke is dan verplicht om alle persoonsgegevens van de inwoner bij elkaar te verzamelen en te verstrekken. Met een geautomatiseerde zoekfunctionaliteit kan binnen gemeentelijke informatiesystemen gezocht worden op een specifieke zoekterm, bijvoorbeeld de naam en voorletters van de verzoeker. Het resultaat dat zichtbaar wordt is de locatie waar persoonsgegevens van de verzoeker zich bevinden. Werknemers kan vervolgens gevraagd worden de benodigde informatie aan de privacy officer te verstrekken, zodat deze op het verzoek kan reageren.

Artikel 7 Gebruik elektronische communicatiemiddelen
In dit artikel van het Reglement zijn gedragsregels opgenomen over wat er in de organisatie onder verantwoord e-mail- en internetgebruik wordt verstaan. Een totaal verbod van privégebruik van de elektronische communicatiemiddelen is niet mogelijk. Er kunnen wel beperkende voorwaarden worden gesteld aan het persoonlijk gebruik van de elektronische communicatiemiddelen.

Artikel 8 Controle
Tweede lid
Vanuit beveiligingsoogpunt is het noodzakelijk om e-mail- en internetgebruik te controleren. Het kan dan gaan om het tegengaan van systeemaanvallen door malware en andere schadelijke activiteiten. Hierbij worden inkomende berichten (inclusief bijlagen) en inkomende internetcontent op een geautomatiseerde wijze gecontroleerd. Indien een besmet bericht gevonden wordt, kan dit op een aparte locatie worden bewaard voor nader onderzoek en eventuele herstelwerkzaamheden.

Derde lid
Het voorkomen van onrechtmatig gebruik dan wel misbruik van de elektronische communicatiemiddelen wordt zo veel mogelijk ingebouwd in de software die wordt gebruikt om te e-mailen of te internetten. Vaak zal dit kunnen door content filtering of door het afsluiten van websites of nieuwsgroepen. Ook is het mogelijk om toepassingen volledig af te sluiten door de daarvoor benodigde software zelf niet aan te bieden. Overtreding van het Reglement wordt hierdoor gedeeltelijk onmogelijk gemaakt.

Vierde lid
Indien er sprake is van een redelijk vermoeden van onrechtmatig gebruik of misbruik van de elektronische communicatiemiddelen kan na goedkeuring van de Algemeen Directeur een gerichte controle uitgevoerd worden. Denk hierbij aan de omstandigheden genoemd onder artikel 7 lid 3 en 4 van dit Reglement of bijvoorbeeld aan het doelbewust verstrekken van vertrouwelijke informatie door een werknemer aan onbevoegde derden. De Algemeen Directeur zal de Ondernemingsraad zonder onredelijke vertraging informeren over het inzetten van een gerichte controle. De Algemeen Directeur verstrekt daarbij geen persoonsgegevens aan de Ondernemingsraad en waar passend wordt de melding aan de OR gedaan onder oplegging van vertrouwelijkheid als bedoeld in artikel 20 WOR. Oplegging van vertrouwelijkheid is onder meer passend als de melding op zichzelf weliswaar geen identificerende informatie bevat, maar wanneer uit de context van de melding mogelijk wel afgeleid zou kunnen worden op wie de gerichte controle betrekking heeft.

Vijfde lid
Indien geconstateerd wordt dat een werknemer dit Reglement overtreedt, dan wordt de betrokken werknemer zo spoedig mogelijk hierop aangesproken door de leidinggevende. Hierbij is een bepaalde tijd voor opbouw van het dossier toegestaan indien de omstandigheden daartoe aanleiding geven.

Indien de werknemer op zijn handelen in strijd met het Reglement wordt aangesproken, wordt hij gewaarschuwd voor de (rechtspositionele) gevolgen bij continuering van dit gedrag.

Zesde en zevende lid
Het gebruik van de elektronische communicatiemiddelen door bijvoorbeeld OR-leden, LO-leden, mediators, bedrijfsartsen, andere werknemers met een vertrouwensfunctie en politieke ambtsdragers zijn in beginsel uitgesloten van controle. Dit geldt niet voor de controle ten behoeve van systeem- en netwerkbeveiliging. 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 op de 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. LO-leden bevinden zich in een soortgelijke positie. 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, waarbij men bijvoorbeeld kan denken aan het lekken van geheime c.q. vertrouwelijke stukken.

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 ook hier geen absoluut verbod. 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.

Artikel 9 Bewaartermijn
Dit artikel bevat de bewaartermijn van persoonsgegevens die worden verwerkt in het kader van controle op gebruik van elektronische communicatiemiddelen.

Artikel 10 Rechten van de werknemer en politieke ambtsdragers
In dit artikel worden de rechten van de werknemers en politieke ambtsdragers bij het verwerken van persoonsgegevens behandeld. Transparantie is een belangrijk beginsel voor privacybescherming. Met dit Reglement wordt voldaan aan de informatieplicht op grond van de artikelen 13 en 14 AVG. Daarnaast hebben de werknemers en politieke ambtsdragers de rechten genoemd in artikel 15 t/m 22 AVG, waaronder een inzage- en rectificatierecht en het recht om een klacht in te dienen bij de Autoriteit Persoonsgegevens.

Artikel 11 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.

Artikel 12 Onvoorziene omstandigheden
Bij onvoorziene omstandigheden beslist de verwerkingsverantwoordelijke.

Artikel 13 Openbaarmaking, inwerkingtreding en evaluatie
Het Reglement dient helder naar de werknemers en politieke ambtsdragers te worden gecommuniceerd. De werknemers 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 Reglement.

Het Reglement kan bijvoorbeeld naast verstrekking op papier, tevens toegankelijk zijn via het P&O handboek op intranet. Op die manier is verzekerd dat men zich bewust is van de inhoud van het Reglement.

Dit Reglement wordt vierjaarlijks geëvalueerd door de verwerkingsverantwoordelijke en de Ondernemingsraad.