gemeente lingewaard

GEMEENTEBLAD

Officiële uitgave van de gemeente Lingewaard

Nr. 243496

8 oktober

2019

Besluit van het college van burgemeester en wethouders van de gemeente Lingewaard houdende regels omtrent internet- en emailgebruik (Regeling bij internet- en emailgebruik gemeente Lingewaard)

Inhoudsopgave

Artikel 1 Begripsbepaling

Voor de toepassing van deze regeling wordt verstaan onder:

a. **werkgever:**
Burgemeester en wethouders van gemeente Lingewaard.

b. **medewerker:**
De werknemer zoals bedoeld in artikel 1:1 lid 1 sub a CAR-UWO.

Artikel 2 Uitgangspunt

Lid 1

Gegevens die tot een persoon herleidbaar zijn zullen niet worden geregistreerd, verzameld, gecontroleerd, gecombineerd dan wel bewerkt worden, anders dan in deze regeling is afgesproken.

Lid 2

Persoonlijke gegevens zullen alleen gebruikt worden voor het doel waarvoor ze verzameld zijn.

Lid 3

Het registreren van gegevens die tot een persoon herleidbaar zijn wordt tot het minimum beperkt. Hierbij wordt gestreefd naar een maximale bescherming van de privacy van medewerkers op de werkplek.

Artikel 3 Email-gebruik

Lid 1

Medewerkers zijn gerechtigd het emailsysteem voor niet-zakelijk verkeer te gebruiken voor het ontvangen en versturen van persoonlijke mailberichten zowel intern als extern, mits dit niet storend is voor hun dagelijkse werkzaamheden.

Lid 2

Het recht van de medewerker om mailberichten te ontvangen en versturen is gebonden aan de volgende voorwaarden:

a. Het is niet toegestaan kettingbrieven te versturen, dreigende, seksueel intimiderende, dan wel racistische berichten te versturen.
b. Het is niet toegestaan om software te verzenden of op te vragen.
c. Er wordt terughoudend omgegaan met het verzenden van persoonsgegevens aan derden. Mocht dit nodig zijn dat kan dit in overleg met het team IV met een beveiligde voorziening worden gedaan.

Lid 3

Iedere medewerker dient bij inkomende berichten alert te zijn op mogelijke virussen; bij twijfel direct de servicedesk van team Informatievoorziening (IV) waarschuwen.

Lid 4

Bij afwezigheid van de medewerker kan een collega het recht krijgen om de binnengekomen e-mailberichten van de medewerker te lezen op relevantie.

Lid 5
De werkgever zal niet zonder reden de inhoud van e-mailberichten van de medewerker lezen. Eveneens zullen persoonsgegevens omtrent het aantal e-mails, de e-mailadressen en andere data hieromtrent niet actief gecontroleerd worden. Dit laat onverlet dat controles op incidentele basis vanwege een zwaarwichtige reden kunnen plaatsvinden.

Lid 6
De direct leidinggevende kan via het team IV een aanvraag doen de emailbox van een medewerker toegankelijk te maken voor collega's.

Lid 7
De direct leidinggevende informeert betrokken medewerker zoals bedoeld in lid 6. van dit artikel tenzij dit vanwege ziekte of anders onmogelijk is.

Artikel 4 Internetgebruik

Lid 1
Medewerkers zijn gerechtigd het internetsysteem voor niet- zakelijk verkeer te gebruiken, mits dit niet storend is voor hun dagelijkse werkzaamheden.

Lid 2
Het is niet toegestaan sites te bezoeken die
a. pornografisch materiaal bevatten
b. racistisch van aard zijn
c. on-line gokken faciliteren
d. aanzetten tot haat en geweld

Lid 3
Het is niet toegestaan om illegale en/of legale software te downloaden. Indien bepaalde bestanden of programma's nodig zijn voor het werk, neemt de medewerker contact op met de adviseur van het team IV.

Artikel 5 Reconstructie internetgebruik
De gemeente Lingewaard legt geen gerichte administratie aan van het individuele internetgebruik van medewerkers. De gemeente is echter wel in staat het internetgebruik van een medewerker te reconstrueren uit logging die door de betrokken systemen wordt vastgelegd.

Artikel 6 Controle
Lid 1
Controle op het gebruik van de email en internet vindt plaats:

a. Voor verkeersgegevens (tijd, hoeveelheid, omvang). Alleen bij zwaarwegende redenen vindt controle op de inhoud plaats.
b. Ter voorkoming van onrechtmatig gebruik dan wel misbruik.
c. Geanonimiseerd en steekproefsgewijs.
d. In het kader van het beveiligen van het systeem en het netwerk voor het tegengaan van virussen en andere schadelijke programma's.

Lid 2
Controle vindt plaats op het niveau van getotaliseerde gegevens die niet herleidbaar zijn tot individuele personen. Indien een medewerker of een groep medewerkers wordt verdacht van het overtreden van regels, kan gedurende een vastgestelde (korte) periode gerichte controle plaatsvinden.

Lid 3
Onrechtmatig gebruik dan wel misbruik van de email en internet wordt zo veel mogelijk softwarematig onmogelijk gemaakt.

Lid 4
Indien geconstateerd wordt dat een medewerker dit reglement overtreedt, wordt hij daarop zo spoedig mogelijk ter verantwoording geroepen door zijn/haar leidinggevende.

Lid 5

Het gebruik van de email en internet door leden van de ondernemingsraad, leden van het georganiseerd overleg in ambtenarenzaken, interne vertrouwenspersonen en bedrijfsartsen is in beginsel uitgesloten van controle.

Lid 6
(Heimelijke) observatie van internet- en e - mailgebuik is incidenteel toegestaan. Er moet echter wel sprake zijn van een redelijke verdenking of vermoeden van een strafbaar feit of ongeoorloofde handeling t.a.v. één of meerdere medewerkers die een dergelijke inzet rechtvaardigen. Hierbij is vereist dat andere middelen zijn uitgeput en dat een zwaarwichtig belang van de organisatie in het geding is. Het moet in de organisatie bekend zijn dat in uitzonderlijke situaties computergebruik wordt gemonitord en welk gedrag niet wordt getolereerd.

Lid 7
Indien er een redelijk vermoeden bestaat van onrechtmatig gebruik, dan wel misbruik van computergebruik door betrokkene, kan dit worden gemeld bij het directieteam die vervolgens opdracht geeft aan de systeembeheerder om het email en internet gebruik vast te leggen en te verstrekken aan betrokkene zoals genoemd in artikel 7 van deze regeling.

Artikel 7 Personen aan wie persoonsgegevens wordt verstrekt
De vastgelegde controle op persoonsgegevens worden, op verzoek, verstrekt aan:
a. Het directieteam, om inzicht te verkrijgen in de mate van gebruik van de computer (e-mail en internet). Het betreft hier dan slechts gegevens, in niet tot de persoon herleidbare vorm.
b. De verantwoordelijke, indien er een redelijk vermoeden bestaat van onrechtmatig gebruik dan wel misbruik zoals genoemd in artikel 6 lid 6 en 7 van deze regeling.
c. Degene die op verzoek van de verantwoordelijke is (zijn) belast met of leiding geeft aan onderzoek naar onrechtmatig misbruik van de computer zoals genoemd in artikel 6 lid 6. en 7. van deze regeling.

Artikel 8 Bewaring en verwijdering
Lid 1
Persoonsgegevens over e – mail- en internetgebruik worden niet langer bewaard dan noodzakelijk met een maximum bewaartermijn van 6 maanden.

Lid 2
Gegevens die ouder zijn dan zes maanden worden automatisch verwijderd, tenzij er bijzondere redenen zijn, bijvoorbeeld een zwaarwegend vermoeden van onrechtmatig gebruik dan wel misbruik, om de gegevens langer te bewaren. Dat moet dan expliciet kunnen worden gemaakt en worden gemeld aan het Cbp.

Lid 3
Indien de systeembeheerder om technische redenen persoonsgegevens niet kan verwijderen, wordt onder verwijderen verstaan het niet meer verstrekken van deze en indien mogelijk deze afschermen.

Artikel 9 Onvoorziene gevallen
In gevallen waarin deze regeling niet of niet in redelijkheid voorziet, kan de werkgever een bijzondere voorziening treffen.

Artikel 10 Citeertitel en inwerkingtreding
Deze regeling kan worden aangehaald als de “Regeling bij internet- en emailgebruik gemeente Lingewaard” en treedt in werking met ingang van 1 januari 2017. Vanaf de inwerkingtredingdatum van deze regeling vervalt de regeling Privacyreglement d.d. 1-08-2003.

Algemene en artikelsgewijze toelichting

Inhoudsopgave

Algemeen

Burgers verlangen een integere overheid. Om deze reden is iedere overheidsorganisatie wettelijk verplicht integriteitsbeleid te voeren en zich daarover te verantwoorden. In de Ambtenarenwet (Aw) is vorm en inhoud gegeven aan een integere overheid en het integer handelen van hun medewerkers. Het gaat hierbij om:

- het afleggen van de eed of belofte;
- het melden, registreren en verbieden van bepaalde nevenfuncties;
- het openbaar maken van nevenfuncties;
- het melden van financiële belangen en
- de noodzaak van een procedure voor de klokkenluiders.

In de CAR-UWO zijn mede daarom de volgende maatregelen ten aanzien van de ambtelijke integriteit bepaald.

- Afleggen eed of belofte (artikel 15:1a);
- Persoonlijk gebruik van goederen of diensten (artikel 15:1b);
- Geheimhouding tijdens en na beëindiging van het dienstverband (artikel 15:1b, lid c)
- Aannemen van geschenken en gelden (artikel 15:1c);
- Huisregels/ gedragscode (artikel 15:1 en 15:1d);
- Nevenwerkzaamheden (artikel 15:1e);
- Melding financiële belangen (artikel 15:1f);
- Inkoop (artikel 15:1g) en
- Vermoeden misstanden (artikel 15:2).

Deze regeling gaat in op het persoonlijk gebruik van goederen of diensten en dan specifiek op het gebruik van e-mail en internet. Binnen de gemeente Lingewaard wordt veel gebruik gemaakt van e-mail en internet. Uit onderzoek naar rechtspraak over e-mail- of internetmisbruik blijkt dat de aanwezigheid van een gedragscode zeer relevant is. Het is voor de gemeente dan ook zaak daarover een duidelijk beleid te voeren. Elektronische controle van computergebruik raakt echter het terrein van de bescherming van de persoonlijke levenssfeer van de medewerker. Op het controleren van het gebruik van e-mail en internet op de werkplek is daarom de Wet bescherming persoonsgegevens (WBP) van toepassing die op 1 september 2001 in werking is getreden.

Het controleren van e-mail- en internetgebruik is een zogenaamd personeelvolgsysteem. Voor de invoering van een personeelvolgsysteem en een privacyreglement is op grond van artikel 27, eerste lid, onder k en l, van de Wet op de ondernemingsraden, de instemming van de ondernemingsraad (OR) vereist. Dit geldt ook voor een eventuele latere wijziging of bij intrekking van het reglement. Na instemming van de OR kan het reglement op de voor gemeenten gebruikelijke wijze worden vastgesteld en ingevoerd.
Een verantwoordelijke1 is verplicht om de verwerking van persoonsgegevens te melden bij het College bescherming persoonsgegevens (Cbp) voordat hij begint met de verwerking. In het zogenaamde Vrijstellingsbesluit staan eisen geformuleerd waaraan de verwerkingen moeten voldoen, wil de vrijstelling van de meldingsverplichting daadwerkelijk gelden. Op basis van het Vrijstellingsbesluit valt controle op het gebruik van e-mail en internet onder de vrijstelling mits voldaan wordt aan de vereisten van het Vrijstellingsbesluit.
Deze vereisten houden in dat geen andere persoonsgegevens worden verwerkt dan:

1. gegevens ten behoeve van identificatie van en communicatie (username en toegangscode) met de gebruikers binnen het netwerk;
2. gegevens met betrekking tot bevoegdheden van de gebruikers en de netwerkbeheerders met het oog op de aangeboden faciliteiten en diensten van het netwerk;
3. gegevens met betrekking tot de verrichtingen van de gebruikers en netwerkbeheerders en
4. gegevens met betrekking tot elektronische berichten van of voor de gebruikers.

Daarnaast geldt dat de persoonsgegevens slechts worden verstrekt aan degenen die belast zijn met de interne controle en beveiliging (de doeleinden van de verwerking), met dien verstande dat verstrekking slechts geschiedt met het oog op het behandelen van geschillen. Bovendien dienen de persoonsgegevens uiterlijk zes maanden nadat ze zijn verkregen te worden verwijderd. Ten slotte geldt dat de OR aan de controle instemming heeft verleend.

Artikel 1
Van persoonsgegevens is sprake als de identiteit van de persoon op wie de informatie betrekking heeft ook redelijkerwijs vastgesteld kan worden. Het feit dat de naam van de betrokkene niet aan de gegevens gekoppeld is maakt niet altijd uit. Zo is met behulp van een personeelsnummer of een login-naam een medewerker te traceren. Getotaliseerde gegevens van het gehele personeelsbestand of een team met een redelijke omvang vallen niet onder deze regeling.

Artikel 3 en artikel 4

Het persoonlijk internet- en emailgebruik kan aan bepaalde voorwaarden worden verbonden. Het is mogelijk de lijst van voorwaarden, in overleg tussen bestuurder en ondernemingsraad, in te korten dan wel uit te breiden.
Het gebruik van internet en email kan storend werken.

- Direct storend door het bezoeken van sites in de omgeving waar collega's daar hinder van kunnen hebben
- Indirect storend als er (tijdelijk) minder werk wordt uitgevoerd doordat er (teveel) tijd aan het privé internetten of mailen wordt besteed

Met name het signaleren en het bespreekbaar maken van een collega die indirect stoort is een aandachtspunt dat bij de implementatie van de regeling aandacht moet krijgen. Tevens hoe de teamleider gefaciliteerd kan worden om dit bespreekbaar te maken met de betreffende medewerker dan wel met medewerkers die het indirect storend gebruik van een collega ervaren.
Langdurige afwezigheid kan zijn ziekte of uitdiensttreding. Waar de voortgang van de werkzaamheden van de langdurige afwezige is het noodzakelijk eventuele emailadressen te kunnen benaderen om te lezen. Tevens kan de afwijzigheidsassistent worden aangezet, waarin kan worden verwezen naar een andere contactpersoon binnen de gemeente.

Artikel 5
Een reconstructie van internetgebruik kan bijvoorbeeld gevraagd worden indien er een vermoeden van misstand is. Hiervoor is de Regeling Melding Vermoeden Misstand van toepassing.

Artikel 6
Vastgelegde gegevens (na bewerking) kunnen worden verstrekt aan de teammanager informatievoorziening voor het verkrijgen van inzicht in de mate van gebruik van email en internet. Voor het verkrijgen van inzicht in de mate van gebruik zal in het kader van kosten- en capaciteitsbeheersing de controle beperkt blijven tot verkeersgegevens.

De genomen maatregelen dienen in redelijke verhouding te staan tot de belangen van de medewerker en de gebruikte middelen mogen niet een verdergaande inbreuk maken op die belangen dan strikt noodzakelijk is (proportionaliteit en subsidiariteit). Steeds zal hiertoe een belangenafweging moeten plaatsvinden. Het doel rechtvaardigt dus niet een continue controle en de daarmee gepaard gaande verregaande inbreuk op de persoonlijke levenssfeer van de werknemer. Controle op naleving zal daarom steekproefsgewijs geschieden.
Het is in het algemeen niet noodzakelijk om aan de teammanager informatievoorziening rapportages en gebruiksstatistieken van het e-mail- en internetgebruik van de medewerkers op persoonsniveau te verstrekken. De gegevens in de rapportages en statistieken zullen dus meestal ontdaan kunnen worden van hun identificerende kenmerken. Alleen als er concrete verdenkingen bestaan tegen een bepaalde medewerker, is rapportage op persoonsniveau noodzakelijk en dan ook toegestaan. Individueel volgen van een medewerker wordt na afloop aan de medewerker gemeld met vermelding van de redenen daartoe en de resultaten van het volgen.

Een bepaalde tijd voor opbouw van het dossier is toegestaan, indien de omstandigheden daartoe aanleiding geven. Een medewerker die in strijd handelt met het de regeling internet en emailgebruik wordt eerst schriftelijk door de verantwoordelijke gewaarschuwd. Continuering van dit gedrag heeft rechtspositionele gevolgen. Dit gedrag wordt beschouwd als plichtsverzuim.
Deze bepaling betreft de communicatie per e-mail van leden van de OR ten behoeve van hun OR-werkzaamheden. Op grond van artikel 17 Wet Ondernemingsraden (WOR) hebben zij het recht om onderling te overleggen met gebruik van voorzieningen waarover het OR-lid als zodanig kan beschikken. De wetsgeschiedenis van artikel 17 WOR maakt helder dat tussen de OR en de werkgever geen gezagsrelatie bestaat. De werkgever kan zijn gezagsbevoegdheid dus niet aanwenden om het e-mailgebruik van OR-leden in functie te controleren. Dit betekent dat op e-mail van, aan en tussen OR-leden in functie de algemene wettelijke regels omtrent vertrouwelijke communicatie van toepassing zijn. In het LOGA d.d. 23 december 2004 is geconcludeerd dat GO-leden (GO: Georganiseerd Overleg) zich in een soortgelijke positie bevinden. Om die reden is besloten de gedragslijn voor OR-leden ook te hanteren voor GO-leden. Daarmee is dit soort e-mail geprivilegieerd en mag de werkgever er in beginsel geen kennis van nemen. Het betreft hier echter geen absoluut verbod. Er kan van worden afgeweken in bepaalde situaties van plichtsverzuim, zoals geregeld in artikel 16:1:1, tweede lid van de Uitwerkingsovereenkomst (UWO), waarbij men bijvoorbeeld kan denken aan het lekken van geheime c.q. vertrouwelijke stukken. Daarnaast ziet deze bepaling ook toe op het gebruik van internet. Het Cbp heeft de VNG in een brief d.d. 22 september 2004 laten weten dat artikel 6, zesde lid niet alleen geldt voor het gebruik van e-mailfaciliteiten, maar ook voor internetgebruik. Dit standpunt van het Cbp heeft de VNG in haar privacyreglement verwerkt, maar is nog niet opgenomen in de 'Raamregeling voor het gebruik van e-mail en internet' van het Cbp.

Artikel 8
Het is in het algemeen niet nodig om de persoonsgegevens lang te bewaren. De standaardtermijn is daarom zes maanden. In het geval van een zwaarwegend vermoeden van onrechtmatig gebruik dan wel misbruik, worden de gegevens uit die zes maanden bewaard. Zodra een nader onderzoek is afgerond en dit niet leidt tot maatregelen worden de gegevens verwijderd.
In relatie tot de termijn gedurende welke persoonsgegevens mogen worden bewaard, kan het volgende worden opgemerkt. De termijn gedurende welke de in archiefbescheiden opgenomen persoonsgegevens mogen worden bewaard, is in beginsel onbepaald. Deze onbepaalde termijn houdt direct verband met het doeleinde waarvoor de gegevens worden bewaard: behoud van (een deel van) het Nederlandse culturele erfgoed.
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).

Voetnoten:
1: De Wbp definieert de verantwoordelijke als degene die het doel en de middelen voor de verwerking van persoonsgegevens vaststelt. De Wbp legt aan de verantwoordelijke een aantal verplichtingen op. Er kunnen bij een verwerking meerdere verantwoordelijken zijn.