PURMEREND

GEMEENTEBLAD

Officiële uitgave van de gemeente Purmerend

Nr. 256428

22 oktober 2019

Reglement Veilig gegevensgebruik en Privacy gemeente Purmerend 2019

Burgemeester en wethouder van Purmerend,

Gelet op:
- Artikel 32 lid 4 van de Algemene Verordening Gegevensbescherming (AVG);
- Maatregel 7.1.2.1; 7.2.2.1; 8.1.3.1; 8.1.3.2 en 9.4.2.1 van de Baseline Informatiebeveiliging Overheid (BIO- versie 1.0.3);
- De brief van de Ondernemingsraad van 26 september 2019 (kenmerk 2019-16) houdende de instemming met het voorgenomen besluit Reglement Veilig Gegevensgebruik en Privacy 2019

BESLUITEN:

1. Het *Reglement Veilig gegevensgebruik en Privacy Gemeente Purmerend 2019* vast te stellen.
2. Het *Privacyreglement telefoon-, e-mail en internetgebruik voor de gemeente Purmerend 2004* gelijktijdig in te trekken met de in werking treding van dit reglement.

1. Doel
Dit reglement heeft als doel regels te stellen en de medewerker te informeren over:
1. Wat van de medewerker wordt verwacht ten aanzien van het veilig omgaan met gegevens die door of via de gemeente verwerkt worden bij het uitoefenen van zijn/haar werkzaamheden en de daarvoor beschikbaar gestelde faciliteiten.
2. Hoe daarbij rekening wordt gehouden met de privacy van de medewerker.

2. Uitgangspunten
1. De gemeente stelt aan de medewerker faciliteiten beschikbaar om gegevens te verwerken en te gebruiken bij de uitvoering van zijn/haar werkzaamheden voor de gemeente.
2. Deze faciliteiten zijn niet bestemd voor eigen zakelijke activiteiten van de medewerker.
3. Binnen de hieronder genoemde grenzen mag hij/zij deze faciliteiten wel gebruiken voor zijn/haar eigen persoonlijke activiteiten.
4. Dit reglement is zowel van toepassing op de fysieke werkplek in de kantoren van de gemeente als op het elders werken met de faciliteiten van de gemeente (plaatsonafhankelijk werken).

3. Relatie met Gedragscode voor medewerkers van de gemeente Purmerend 2018
Dit reglement hangt samen met de gedragscode en in het bijzonder:
- Thema 4: Regels over het omgaan met informatie.
- Thema 5: Regels over het gebruik van bedrijfsmiddelen.

4. Begrippen
1. *Medewerker:* een ieder die toegang krijgt tot de informatiehuishouding van de gemeente voor werkzaamheden in opdracht van en/of voor de gemeente. Een medewerker kan iemand zijn die in dienst is bij een andere organisatie.
2. *Netwerkaccount:* de unieke (persoonsgebonden) toegangsgegevens tot het netwerk van de gemeente.
3. *Applicatieaccount:* de unieke (persoonsgebonden) toegangsgegevens tot een informatiesysteem (applicatie).
4. *Applicatie:* een toegepast informatiesysteem. Zogeheten “app’s” worden hier gelijkgesteld met applicaties.
5. *E-mailaccount:* het unieke e-mailadres dat gekoppeld is aan het e-maildomein van de gemeente. Het regelt ook de toegang tot en het gebruik van agenda’s.
6. *Logging:* het automatisch registreren van gebruikshandelingen op het netwerk, met en binnen applicaties, e-mail en telefonie. Logging is een noodzakelijke beveiligingsmaatregel om te kunnen controleren wie welke handelingen heeft uitgevoerd dan wel fouten op te sporen en/of te herstellen.

7. *Monitoring:* het (op afstand) bewaken van locaties, systemen en/of processen (in veel gevallen maar niet uitsluitend door middel van beeld en/of geluid). Monitoring is noodzakelijk om te kunnen controleren wie welke handelingen heeft uitgevoerd dan wel aanwezig is geweest op specifieke locaties.
8. *Tracking:* het volgen van mensen door het volgen van hun mobiele apparatuur.
9. *Informatiehuishouding:* het geheel van onder meer applicaties, programmatuur, processen, gegevens, koppelingen, diensten van derden, documenten en bestanden.
10. *Verwerken van gegevens:* alle handelingen met gegevens zoals het maken, raadplegen, opslaan, vernietigen, verzenden en ter beschikking stellen van gegevens.
11. *Kwalijke inhoud:* het hebben, bekijken, downloaden, verspreiden of versturen van bestanden met pornografische, racistische, discriminerende, beledigende, aanstootgevende of (seksueel) intimiderende teksten en afbeeldingen, dan wel die (kunnen) aanzetten tot haat en/of geweld, zoals bedoeld in regel 5.3 van de Gedragscode, alsmede online gokken.
12. *Mobile Device Management (MDM):* het op afstand beheren door of namens de gemeente van mobiele apparatuur. Dat omvat onder meer het wissen van gegevens, het installeren van software en het bepalen van de geografische locatie van de apparatuur.

5. Netwerkaccount

1. De medewerker krijgt een netwerkaccount om bij de uitvoering van zijn/haar werkzaamheden voor de gemeente gebruik te kunnen maken van de informatiehuishouding van de gemeente.
2. Door middel van het netwerkaccount krijgt hij/zij toegang tot informatiesystemen en gegevens voor zover dat past bij het uitvoeren van zijn/haar werkzaamheden.
3. Het netwerkaccount bestaat uit een unieke gebruikersnaam, wachtwoord en eventueel extra inloggegevens (bijvoorbeeld tijdelijke code die via SMS wordt toegezonden).
4. Het netwerkaccount is persoonlijk en mag niet gedeeld worden met anderen.
5. Het netwerkaccount wordt gedeactiveerd direct na beëindiging van de werkzaamheden voor de gemeente. Binnen een halfjaar daarna wordt het verwijderd.
6. De gemeente heeft het recht om bij (vermoedens van) integriteitsschendingen de toegang tot het netwerk in te trekken. Hierover oordeelt de Algemeen Directeur.

6. Applicaties (informatiesystemen)

1. De medewerker krijgt toegangsrechten tot die applicaties/informatiesystemen die hij/zij nodig heeft bij de uitvoering van zijn/haar werkzaamheden. Dit kan zowel betrekking hebben op applicaties binnen het gemeentelijk netwerk als op applicaties die de gemeente als dienst afneemt van leveranciers of ketenpartners.
2. Het applicatieaccount regelt de rechten van de gebruiker binnen de applicatie.
3. Persoonsgebonden applicatieaccounts mogen niet worden gedeeld met anderen.
4. Niet persoonsgebonden applicatieaccounts mogen alleen worden gedeeld met anderen waarvan bekend is dat zij toegangsrechten hebben.
5. Applicatieaccounts worden gewijzigd of gedeactiveerd na wijziging of beëindiging van de werkzaamheden.
6. De gemeente heeft het recht om bij (vermoedens van) integriteitsschendingen de toegang tot applicaties in te trekken. Hierover oordeelt de Algemeen Directeur.

7. Raadplegen van gegevens over personen

Het raadplegen van gegevens over personen is alleen toegestaan voor zover het ***noodzakelijk*** is voor de uitvoering van de opgedragen werkzaamheden.
Let op: Steeds meer informatiesystemen maken gebruik van koppelingen met andere bronsystemen (bijvoorbeeld de Basisregistratie Personen) om gegevens op te halen. Ook die gegevens mogen uitsluitend gebruikt worden voor de specifieke opdracht waaraan uitvoering gegeven wordt.

8. Logging en monitoring

1. Logging en monitoring gebeurt op diverse plaatsen en momenten: bijvoorbeeld bij de toegang tot, het gebruik van en het afsluiten van het netwerk, applicaties, gebouwen en terreinen.
2. De gemeente bewaart de gegevens van logging en monitoring (bijv. documenten, registraties en camerabeelden) niet langer dan nodig is om de doelen te realiseren waarvoor deze gegevens worden verzameld.
3. De gemeente gebruikt logging en/of monitoring niet om individuele werkprestaties te monitoren.
4. De gemeente kan bij (vermoedens van) integriteitsschendingen gebruik maken van deze gegevens bijvoorbeeld voor forensisch onderzoek. Hierover oordeelt de Algemeen Directeur.

9. Diensten van derden

1. Voor de uitvoering van werkzaamheden mag de medewerker alleen gebruik maken van diensten van derden waarmee de gemeente een zakelijke overeenkomst is aangegaan en/of die zijn vermeld op de lijst met toegestane digitale diensten. Het is de medewerker zonder mandaat niet toegestaan om daarvoor zelf overeenkomsten aan te gaan (bijvoorbeeld: het laten maken van websites en apps). Het is evenmin toegestaan om een gebruikersaccount aan te maken als deze dienst niet voorkomt op de lijst met toegestane digitale diensten.
2. Het gebruik van diensten voor de verzending vanuit de gemeente en opslag van gegevens, documenten en/of bestanden (al dan niet gratis) zoals WeTransfer, Dropbox, Googledrive en Trello is niet toegestaan, tenzij deze voor komen op de lijst met toegestane digitale diensten. De gemeente stelt daarvoor alternatieven beschikbaar, zoals Sharefile en Onedrive.
3. De Algemeen Directeur stelt de lijst met toegestane digitale diensten vast.

10. Digitale werkplek

1. Gegevens die de medewerker gebruikt of opslaat bij de uitvoering van zijn/haar werkzaamheden worden opgeslagen binnen de desbetreffende applicaties, het document managementsysteem of de gemeenschappelijke opslaglocaties (bijvoorbeeld: G- en L- schijf). De eigen werkdocumenten (bijvoorbeeld concept verslag personeelsgesprek, persoonlijke werkaantekeningen) kan de medewerker opslaan binnen de persoonlijke digitale werkplek. Bijvoorbeeld de M-schijf, het Sharefile Webportaal en Onedrive.
2. Het is niet toegestaan om bestanden met kwalijke inhoud en/of materiaal dat auteursrechtelijk beschermd is zonder toestemming van rechthebbende op te slaan.
   Een uitzondering kan voortvloeien uit de aard van de functie (bijv. buitengewoon opsporingsambtenaar, CISO, systeembeheerder) als de te verrichten werkzaamheden dit vereisen.
3. Voorafgaande aan de beëindiging van zijn/haar werkzaamheden ruimt de medewerker de persoonlijke digitale werkplek op. Dat wil zeggen: belangrijke documenten ter archivering aanbieden bij DIV en onbelangrijke documenten vernietigen. Bij twijfel altijd contact opnemen met DIV.
4. Vanaf het moment dat de medewerker niet meer werkzaam is voor de gemeente, heeft de gemeente het recht om de persoonlijke digitale werkplek van de medewerker te raadplegen.
5. Gelijktijdig met het verwijderen van het netwerkaccount van een medewerker worden de bestanden in de persoonlijke digitale werkplek verwijderd.
6. De gemeente zal anderen (ook leidinggevenden) geen toegang geven tot de persoonlijke digitale werkplek van de medewerker, tenzij er sprake is van plotselinge uitval van de medewerker en er dringend behoefte is aan de inhoud. Hierover beslist de Domeindirecteur van de betrokken medewerker. Ingeval van (vermoedens van) integriteitsschendingen beslist de Algemeen Directeur.

11. Persoonlijk e-mailaccount en agenda

1. Een medewerker die een netwerkaccount heeft, krijgt doorgaans ook een persoonlijk e-mailaccount en agendafaciliteiten.
2. Het e-mailaccount mag niet gedeeld worden met anderen.
3. Een e-mailaccount wordt gedeactiveerd na beëindiging van de werkzaamheden. Binnen een half jaar daarna wordt het verwijderd.
4. Het e-mailaccount behoort tot het privédomein van de medewerker. De medewerker bepaalt dan ook wie hij daar toegang toe geeft. Bijvoorbeeld door het machtigen van collega('s) tot inzage met behulp van de mogelijkheden binnen de applicatie.
5. De gemeente zal anderen (ook leidinggevenden) geen toegang geven tot de e-mailbox van de medewerker, tenzij er sprake is van plotselinge uitval van de medewerker en er dringend behoefte is aan de inhoud. Hierover beslist de Domeindirecteur van de betrokken medewerker. Ingeval van (vermoedens van) integriteitsschendingen beslist de Algemeen Directeur.
6. De medewerker is er verantwoordelijk voor dat daartoe bestemde e-mailberichten worden gearchiveerd in de daarvoor bestemde systemen en hoort deze ter archivering aan te bieden bij het team DIV.
7. Voorafgaande aan beëindiging van de werkzaamheden ruimt de medewerker zijn/haar e-mailbox op. Dat wil zeggen: daartoe bestemde e-mailberichten archiveren en overige e-mailberichten vernietigen.
8. Vanaf het moment dat hij/zij de werkzaamheden voor de gemeente heeft beëindigd, hebben de direct leidinggevende van de medewerker en de teammanager ICT het recht om de e-mailbox van de medewerker te raadplegen, indien dit noodzakelijk is voor het onbelemmerd voortzetten van de werkzaamheden.

12. E-mailgebruik

1. E-mailvoorzieningen zijn er ten dienste van de werkzaamheden voor de gemeente. Het gebruik daarvan voor privédoeleinden is toegestaan binnen het redelijke.
2. Het is niet toegestaan om met gemeentelijke faciliteiten eigen commerciële activiteiten te ontplooien.
3. Het gebruik van privé e-mailaccounts voor werkzaamheden ten behoeve van de gemeente is niet toegestaan.
4. E-mailberichten van belangrijke aard die de medewerker verzendt of ontvangt bij de uitvoering van zijn/haar taken worden opgeslagen binnen de desbetreffende applicaties, het document managementsysteem of de gemeenschappelijke opslaglocaties (bijvoorbeeld: G-schijf en L-schijf). Dit geldt in elk geval voor e-mailberichten waarin rechten en verplichtingen van de gemeente worden vastgelegd.
5. Vertrouwelijke berichten worden alleen verstuurd met middelen die de gemeente daarvoor beschikbaar stelt (zoals Sharefile).
6. In het e-mailverkeer worden alleen persoonsgegevens of vertrouwelijke gegevens gebruikt als dat strikt noodzakelijk is.
7. In het e-mailverkeer worden de in het maatschappelijk verkeer gebruikelijke regels van goed fatsoen gehanteerd.

13. Social media

1. Het gebruik van social media (Facebook, Twitter, Instagram, LinkedIn, WhatsApp, et cetera) namens de gemeente is alleen toegestaan in overleg met de teammanager Communicatie. [1]
2. Het gebruik van social media in de communicatie tussen medewerkers is toegestaan, mits deze media voorkomen op de lijst zoals bedoeld in artikel 9 lid 1 en 3. Daarbij wordt een medium gebruikt dat encryptie biedt.
3. Het privégebruik van social media binnen werktijd is in principe toegestaan binnen de grenzen van het redelijke.
4. Het is toegestaan om bij privé accounts te melden werkzaam te zijn voor de gemeente, zolang de medewerker zich niet voordoet als vertegenwoordiger van de gemeente.
5. Bij het gebruik van social media worden de in het maatschappelijk verkeer gebruikelijke regels van goed fatsoen gehanteerd. Dat wil zeggen dat er in ieder geval respectvol met elkaar omgegaan dient te worden.

14. Internetgebruik [2]

1. Het zoeken naar en raadplegen van informatie op het internet is de eigen verantwoordelijkheid van de medewerker. Het is niet toegestaan om met gemeentelijke faciliteiten bewust internetsites te bezoeken die een kwalijke inhoud bevatten.
2. Een uitzondering kan voortvloeien uit de aard van de functie (bijv. buitengewoon opsporingsambtenaar, CISO, systeembeheerder) als de te verrichten werkzaamheden dit vereisen.
3. Het is niet toegestaan om met gemeentelijke faciliteiten eigen commerciële activiteiten te ontplooien.
4. Het staat de medewerker vrij om deel te nemen aan discussiefora op internet en daarbij indien nodig te melden dat hij/zij medewerker is van de gemeente. Het is echter niet toegestaan om zich voor te doen als vertegenwoordiger van de gemeente.
5. Het gebruik van internet vanuit het gemeentelijk netwerk wordt gelogd en gemonitord.

15. Mobiele apparatuur

1. De gemeente stelt mobiele communicatiefaciliteiten beschikbaar voor de uitvoering van werkzaamheden van de gemeente (o.a.: smartphone, tablet).
2. Het beheer van gemeentelijke mobiele apparatuur gebeurt op basis van "mobile device management".
3. De medewerker die eigen mobiele apparatuur gebruikt, dient zelf de kosten van het gebruik te dragen. Indien hij/zij gebruikmaakt van apps die de gemeente beschikbaar stelt, dan staat hij/zij voor die apps beheer op afstand door of namens de gemeente toe.
4. De gemeente zal tracking niet gebruiken, tenzij dit nodig is om vermiste apparatuur terug te vinden en/of te blokkeren.

---

1) Hierop geldt als uitzondering het gebruik van social media door medewerkers Griffie, KCC, Communicatie en de marketingmedewerkers van de Purmaryn.

2) Zie voor opslaan van gegevens van de gemeente ook onder artikel 9 "Diensten van derden".

5. De gemeente hanteert het “zero footprint”- principe [3] :
   5.1. De medewerker gebruikt bij de werkzaamheden voor de gemeente uitsluitend de apps die de gemeente beschikbaar stelt (bijvoorbeeld: Webmail, Sharefile en portaal.purmerend.nl);
   5.2. Het is niet toegestaan om zelf gemeentelijke persoonsgegevens dan wel andere gemeentelijke gegevens die geheim en/of vertrouwelijk van aard zijn op deze apparatuur op te slaan.

6. Bij verlies of diefstal van een mobiel apparaat waarop gemeentelijke apps en/of gegevens staan wordt meteen een melding gemaakt bij het Servicepunt ICT.
7. Voor elke medewerker die een smartphone ter beschikking krijgt gesteld, is een data-abonnement beschikbaar. Het datagebruik is gebaseerd op een fair use policy: voor iedere gebruiker is op maandbasis gemiddeld 1.000 Mb beschikbaar. Zolang het individueel totaal gemiddeld maandgebruik onder die grens blijft, is privégebruik toegestaan.
8. De gemeente heeft het recht om bij (vermoedens van) integriteitsschendingen de mobiele apparatuur in te nemen. Hierover beslist de Algemeen Directeur.

16. Telefonie [4]

1. Het gebruik van telefoonverbindingen wordt geregistreerd om telefoonkosten te kunnen verrekenen met de telefoonprovider.
2. De registratie wordt niet gebruikt om de individuele prestaties van de medewerker te controleren, tenzij er een (vermoeden van) integriteitsschending is.
3. De gevoerde gesprekken worden niet door of namens de gemeente opgenomen. De medewerkers van het KCC beschikken wel over de mogelijkheid om zelf in te stellen dat een gesprek wordt opgenomen.

17. Clean desk en clear screen

De fysieke werkplek bestaat doorgaans uit een bureau en een apparaat dat toegang geeft tot het gemeentelijke netwerk.

1. Clean desk: de werkplek wordt netjes en leeg achtergelaten. Voor papieren documenten geldt het volgende:
   1.1. na afloop van de werktijd opbergen in afsluitbare kasten (lockers);
   1.2 voor zover nodig na behandeling ter archivering bij DIV aanbieden;
   1.3 vernietigbare documenten weggooien in de afsluitbare papierbakken.

2. Clear screen: de medewerker vergrendelt bij het verlaten van de werkplek telkens elk apparaat dat toegang geeft tot het gemeentelijk netwerk. Dit geldt ook bij het plaatsonafhankelijk werken.
3. Bij ontruiming of BHV-oefeningen altijd clear screen toepassen en, voor zover wettelijk verplicht en/of mogelijk, clean desk. Daarbij gaat de persoonlijke, fysieke veiligheid voor op de veiligheid van de gegevens.

18. Persoonlijke kastjes (lockers)

Voor de medewerker die gebruik maakt van een afsluitbaar persoonlijk kastje (locker) van de gemeente geldt het volgende:

1. De gemeente eerbiedigt dit als het privédomein van de medewerker.
2. De gemeente zal anderen (ook leidinggevenden) geen toegang geven, tenzij er sprake is van plotselinge uitval van de medewerker en er dringend behoefte is aan de inhoud. Hierover beslist de (Domein)directeur van de betrokken medewerker. In geval van (vermoedens van) integriteitsschendingen beslist de Algemeen Directeur.

19. Kopieerapparaten, printers en scanners

1. Bij het printen, kopiëren en scannen worden gegevens zowel lokaal op het apparaat als op de netwerkservers opgeslagen.
2. Na het kopiëren, printen of scannen altijd de documenten meenemen.
3. Na het gebruik altijd uitloggen.

20. Consequenties bij niet nakoming

1. Overtreding van dit reglement kan leiden tot maatregelen. Hierover beslist de Algemeen Directeur.

---

3) Het komt nu nog voor dat gemeentelijke apps wel gegevens lokaal op het apparaat opslaan In de nabije toekomst zal er een app gebruikt worden voor veilig e-mailgebruik op mobiele apparaten.

4) Zie ook onder artikel 15: "Mobiele apparatuur".

2. Ten aanzien van het gestelde in artikel 9 lid 1 geldt dat het vorige lid pas in werking treedt twee maanden na eerste publicatie op intranet van de lijst genoemd in artikel 9 lid 3.

21. Onvoorziene omstandigheden

In gevallen waarin dit reglement niet voorziet of bij twijfel omtrent de toepassing van dit reglement, beslist de Algemeen Directeur.

22. Openbaarmaking en evaluatie

1. Dit reglement wordt verstrekt of ter beschikking gesteld via intranet.
2. Dit reglement wordt na twee jaar geëvalueerd door, het college en de ondernemingsraad.

23. Inwerkingtreding en intrekking

1. Dit reglement wordt aangehaald als *Reglement Veilig gegevensgebruik en Privacy gemeente Purmerend 2019*
2. Dit reglement treedt in werking op de dag na publicatie in het gemeenteblad.
3. Het *Privacyreglement telefoon-, e-mail- en internetgebruik Purmerend 2004* wordt ingetrokken per datum inwerkingtreding van dit reglement.

Purmerend, 15 oktober 2019
Burgemeester en wethouders van Purmerend,
de secretaris,
G. Blom
de burgemeester,
D. Bijl