

•

Privacyprotocol

Definitieve versie
2011

Gelet op:

- het feit dat de gemeente Alkmaar aan degenen die bij haar organisatie werkzaam zijn de volgende elektronische- en telecommunicatiemiddelen ter beschikking kan stellen: telefoon, GSM, fax, PC en toebehoren (printer, scanner, kopieermachine) e-mail- en internetfaciliteiten;
- het feit dat de gemeente Alkmaar gebruik maakt van een personeelsvolgsysteem met behulp van toegangspassen ten behoeve van het betreden van gemeentelijke gebouwen door haar medewerkers;
- het feit dat met de genoemde middelen de medewerkers hun functie kunnen uitoefenen;
- het bepaalde in de Wet bescherming persoonsgegevens;
- de op 12 09 2011 verleende instemming met het privacyprotocol door de Ondernemingsraad van de gemeente Alkmaar;

besluit het college van de gemeente Alkmaar het volgende privacyprotocol vast te stellen:

HOOFDSTUK 1 ALGEMENE BEPALINGEN

Artikel 1 Definities

In dit privacyprotocol wordt verstaan dan wel mede verstaan onder:

1. **Wbp:** Wet bescherming persoonsgegevens;
2. **CBP:** College Bescherming Persoonsgegevens;
3. **Gemeente:** de gemeente Alkmaar;
4. **Betrokkene:** de gebruiker van alle ter beschikking gestelde communicatiemiddelen op wie een persoonsgegeven betrekking heeft, alsmede de gebruiker van het personeelsvolgsysteem en die is aan te merken als:
 - a. medewerker in dienst van de gemeente;
 - b. persoon die betaalde of niet-betaalde werkzaamheden voor de gemeente verricht, anders dan in dienstverband;
5. **Verantwoordelijke:** het college van Burgemeester en Wethouders;
6. **Bevoegd gezag:** Gemeentesecretaris/Algemeen directeur;
7. **Beheerder:** Gemeentesecretaris/Algemeen directeur, tevens voorzitter van het AMT;
8. **AMT:** Alkmaars Management Team;
9. **Telecommunicatiemiddelen:** de thans in gebruik zijnde: (mobiele) telefoon, faxapparaat, PC en toebehoren (printer, scanner, kopieermachine)
10. **E-mailfaciliteiten:** de door of namens de gemeente aan medewerkers ter beschikking gestelde e-mailfaciliteiten;
11. **Internetfaciliteiten:** de door of namens de gemeente aan medewerkers ter beschikking gestelde internetfaciliteiten;
12. **Elektronische communicatiemiddelen:** e-mail- en/of internetfaciliteiten;
13. **Persoonsgegevens:** alle gegevens betreffende een geïdentificeerde of identificeerbare natuurlijke persoon in de zin van art. 1 sub a Wbp;
14. **Verkeersgegevens:** gegevens die worden verwerkt voor het overbrengen van communicatie over een elektronisch communicatienetwerk of voor de facturering ervan;
15. **Verwerking 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 in de zin van art. 1 sub b Wbp;

16. **Onrechtmatig gebruik dan wel misbruik van de elektronische communicatiemiddelen:** een doen of nalaten in strijd met dit privacyprotocol of andere wet- en regelgeving of een inbreuk op een recht;
17. **Bestand:** elk, al dan niet geautomatiseerd, gestructureerd geheel van persoonsgegevens, ongeacht of dit geheel van gegevens gecentraliseerd is of verspreid is op een functioneel of geografisch bepaalde wijze, dat volgens bepaalde criteria toegankelijk is en betrekking heeft op verschillende personen;
18. **College:** het college van Burgemeester en Wethouders.

Artikel 2 Reikwijdte

1. Dit privacyprotocol is van toepassing op het verwerken van persoonsgegevens inzake het gebruik van elektronische- en telecommunicatiemiddelen en tevens op het personeelsvolgsysteem. Dit privacyprotocol geeft de wijze weer waarop binnen de gemeente wordt omgegaan met elektronische- en telecommunicatiemiddelen en tevens met gegevens die voortvloeien uit het personeelsvolgsysteem.
2. Dit privacyprotocol geldt voor medewerkers in dienst van de gemeente, personen die betaalde of niet-betaalde werkzaamheden voor de gemeente verrichten, anders dan in ambtelijk dienstverband en politieke bestuurders.

HOOFDSTUK 2 ELEKTRONISCHE- EN TELECOMMUNICATIEMIDDELEN

Par. 1: Doeleinden verwerken persoonsgegevens

Artikel 3 Doeleinden

1. De verwerking van persoonsgegevens met betrekking tot het gebruik van de elektronische en telecommunicatiemiddelen heeft de volgende doeleinden:
 - a. het beveiligen van het systeem en het netwerk tegen virussen, worm-macro's en andere ongewenste invloeden van buitenaf;
 - b. het verkrijgen van inzicht in de mate van gebruik van de elektronische en telecommunicatiemiddelen;
 - c. het voorkomen van onrechtmatig gebruik dan wel misbruik van de elektronische en telecommunicatiemiddelen door betrokkenen;
 - d. het beoordelen van het functioneren van betrokkenen bij verdenking van vermeend misbruik en/of fraude.
2. Persoonsgegevens worden slechts verwerkt voor de uitdrukkelijk van te voren omschreven doeleinden.

Artikel 4 Verwerken van persoonsgegevens

1. Gegevens die herleidbaar zijn tot individuele medewerkers worden slechts verwerkt bij een ernstig vermoeden van onrechtmatig gebruik dan wel misbruik van elektronische en/of telecommunicatiemiddelen. Vastlegging en verwerking vindt slechts plaats in opdracht van de beheerder en na overleg met het sectorhoofd, het afdelingshoofd en de personeelsadviseur.
2. In de vastlegging worden ten hoogste de volgende persoonsgegevens opgenomen:
 - a. gebruikersindicatie, naam, voornaam of voorletters van de medewerker;
 - b. naam van de sector/afdeling waaronder de medewerker valt;

- c. gegevens over de toegang tot de elektronische en/of telecommunicatiemiddelen die door de gemeente Alkmaar is geboden aan de medewerker, inclusief gebruikersnaam, registratienummer, IP-adres;
 - d. gegevens betreffende de datum, het tijdstip, gebruikersidentificatie en de duur van het gebruik van de communicatiemiddelen door de medewerker;
 - e. gegevens betreffende de door de medewerker gebruikte communicatiemiddelen, zoals bezochte internetsites (internet protocoladressen en de webpagina's), gebelde telefoonnummers;
 - f. met betrekking tot het gebruik van e-mail het e-mailadres van de afzender en de geadresseerde, het onderwerp en de inhoud van e-mailberichten en de datum en het tijdstip van verzenden, dan wel ontvangen van e-mailberichten door de medewerker.
3. Indien er een ernstig vermoeden bestaat van onrechtmatig gebruik dan wel misbruik van de elektronische en/of telecommunicatiemiddelen door de medewerker, kan door de beheerder, na overleg met het sectorhoofd, het afdelingshoofd en de personeelsadviseur opdracht worden gegeven om de betreffende gegevens te verstrekken aan de personen bedoeld in artikel 15.

Par. 2: Verantwoordelijkheden en beheer

Artikel 5 Verantwoordelijkheden en beheer

1. Door de verantwoordelijke worden de nodige maatregelen getroffen opdat persoonsgegevens, gelet op de doeleinden waarvoor zij worden verwerkt, juist en nauwkeurig zijn.
2. Bij verdenking van een persoon van onrechtmatig gebruik dan wel misbruik van de elektronische en/of telecommunicatiemiddelen is het niet toegestaan om medewerkers van de gemeente hierover te informeren.
3. Door de verantwoordelijke worden passende technische en organisatorische maatregelen ten uitvoer gelegd om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking.
4. Door de verantwoordelijke worden één of meerdere systeembeheerders en applicatiebeheerders aangewezen die belast zijn met het beheer van het (de) bestand(en). Deze beheerders zijn, op grond van artikel 125a lid 3 Ambtenarenwet, verplicht tot geheimhouding van de persoonsgegevens waarvan zij kennis nemen, behoudens voor zover enig wettelijk voorschrift hen tot mededeling verplicht of uit hun taak de noodzaak tot mededeling voortvloeit.
5. Door het AMT worden voorzieningen getroffen over de positie, integriteit en bevoegdheden van de systeembeheerders, de applicatiebeheerders en de controle daarop. De controle op deze voorzieningen wordt minimaal eenmaal per jaar gedaan door een onafhankelijke instantie, niet zijnde de afdeling I&A en rapporteert aan het bevoegd gezag.

Par. 3: Het gebruik van elektronische- en telecommunicatiemiddelen

Artikel 6 E-mailgebruik

1. De elektronische communicatiemiddelen worden primair gebruikt voor het uitvoeren van de door de gemeente opgedragen taken.
2. Medewerkers van de gemeente mogen incidenteel en kortstondig het e-mailsysteem gebruiken voor het ontvangen en versturen van privé e-mailberichten mits dit gebruik in overeenstemming is met dit privacyprotocol. Dit gebruik mag in geen geval storend zijn voor het computernetwerk of ten koste gaan van het uitvoeren van de aan de betrokkene door de gemeente opgedragen taken.
3. Het is niet toegestaan om:

- a. met behulp van de door de gemeente ter beschikking gestelde e-mailfaciliteiten kettinbrieven of pornografisch materiaal te versturen en/of op te vragen, dan wel aanstootgevende, dreigende, lasterlijke, seksueel intimiderende, onzedelijke, racistische of discriminerende opmerkingen te maken;
- b. met behulp van de door de gemeente ter beschikking gestelde e-mailfaciliteiten illegale software te verzenden en/of op te vragen dan wel bestanden zonder voorafgaand overleg met de systeembeheerders te verzenden of op te vragen waarvan betrokkene redelijkerwijs moet aannemen dat deze te omvangrijk zijn;
- c. e-mails te openen waarvan betrokkenen redelijkerwijs kunnen aannemen dat deze de goede werking van de e-mailfaciliteiten en/of de gegevenssystemen kunnen belemmeren.

Artikel 7 Internetgebruik

- 1. Het gebruik van de internetfaciliteiten wordt in principe primair gebruikt voor het uitvoeren van de door de gemeente opgedragen taken.
- 2. Medewerkers mogen incidenteel en kortstondig het internetsysteem gebruiken voor privé doeleinden mits dit gebruik in overeenstemming is met dit privacyprotocol. Dit gebruik mag in geen geval storend zijn voor het computernetwerk of ten koste gaan van het uitvoeren van de aan de betrokkene door de gemeente opgedragen taken.
- 3. Het is niet toegestaan om:
 - a. met behulp van de door de gemeente ter beschikking gestelde internetfaciliteiten 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, mee te doen in chat-sessies of online te gokken;
 - b. internetsites te bezoeken dan wel software te downloaden waarvan betrokkenen redelijkerwijs kunnen aannemen dat deze de goede werking van de internet faciliteiten en/of de gegevenssystemen kunnen belemmeren.

Artikel 8 Gebruik van (mobiele) telefoon

- 1. Het is niet toegestaan om:
 - a. met behulp van de door de gemeente ter beschikking gestelde telefoon faciliteiten 0900 lijnen, 0906-lijnen, lijnen van prostitutiebedrijven, escortservices te bellen dan wel zonder voorafgaande toestemming van leidinggevenden buitenlandse lijnen te bellen.
- 2. Medewerkers zullen bij het gebruik van alle elektronische en telecommunicatiemiddelen de nodige zorgvuldigheid betrachten en de integriteit en de goede naam van de gemeente waarborgen.
- 3. De registratie van persoonsgegevens worden uitsluitend gebruikt voor de doelstellingen zoals bedoeld in artikel 3.

HOOFDSTUK 3 PERSONEELSVOLGSYSTEEM/TOEGANGSPASSENSYSTEEM

Artikel 9 Doel van het toegangspassensysteem

- 1. Het doel van het toegangspassen is het hebben van een actueel overzicht van welke medewerker zich in het stadhuis of het stadskantoor bevindt.
- 2. Meer specifiek heeft het toegangspassensysteem tot doel:
 - a. Het voorkomen van betreding van de gebouwen door onbevoegden;
 - b. Het bestrijden van fraude;

- c. Het overzichtelijk houden van welke medewerker zich in het stadhuis of het stadskantoor bevindt ten tijde van calamiteiten.

Artikel 10 Verantwoordelijkheden

Het verwerken van persoonsgegevens naar aanleiding van de toegangspassen geschiedt onder verantwoordelijkheid van het college.

Artikel 11 Privacy ten aanzien van de geregistreerde

De registratie van persoonsgegevens wordt uitsluitend gebruikt voor de doelstellingen van het toegangspassensysteem zoals bedoeld in artikel 9.

Artikel 12 Uitgifte van de gegevens die geregistreerd worden

Persoonsgegevens worden verstrekt op mondelinge vordering van de politie of de officier van justitie. Deze vordering dient later schriftelijk te worden bevestigd.

HOOFDSTUK 4 CONTROLE, BEWARING EN VERWIJDERING PERSOONSgegevens

Artikel 13 Controle

1. Controle op e-mail en internetgebruik vindt slechts plaats in het kader van de in artikel 3 lid 1 genoemde doelen. Deze doelen stellen beperkingen aan de omvang en de wijze van controle.
 - a. Controle ter verkrijging van inzicht in de mate van gebruik van de elektronische communicatiemiddelen blijven beperkt tot de verkeersgegevens betreffende de afzender, de bestemming, de datum en de tijd van het bericht.
 - b. Controle ter voorkoming van onrechtmatig gebruik dan wel misbruik van de elektronische communicatiemiddelen wordt zo beperkt mogelijk gehouden, in die zin dat deze in redelijke verhouding staat tot het doel waarvoor deze wordt aangewend. De controle vindt geanonimiseerd en slechts steekproefsgewijs plaats.
 - c. Controle in het kader van 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 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. Voor deze gerichte controle dient toestemming te zijn verleend door de beheerder. Deze gerichte controle wordt slechts uitgevoerd nadat de medewerker is ingelicht dat signalen hierover zijn ontvangen en om zijn reactie is gevraagd. De beheerder 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. Van het besluit tot het verrichten van gerichte controle wordt direct melding gedaan bij de voorzitter van de OR.
3. Controle beperkt zich tot verkeersgegevens van het gebruik van de elektronische communicatiemiddelen. Alleen bij zwaarwegende redenen vindt er controle op de inhoud plaats.
4. Medewerkers die dit privacyprotocol overtreden, worden hierop aangesproken door het sectorhoofd dan wel het betreffende afdelingshoofd.

5. E-mailberichten van OR en GO-leden, bedrijfsartsen, en andere medewerkers met een vertrouwensfunctie zijn in beginsel uitgesloten van controle. Dit geldt niet voor de controle op de veiligheid van het elektronische berichtenverkeer.
6. De verantwoordelijke maakt jaarlijks een rapport op met betrekking tot de frequentie van de individuele controles en overlegt deze rapportage aan de OR.

Artikel 14 Bewaring en verwijdering

1. Persoonsgegevens die gerelateerd zijn aan het toegangspassensysteem worden maximaal één maand bewaard. Persoonsgegevens die gerelateerd zijn aan de communicatiemiddelen worden maximaal drie maanden bewaard. Gegevens die ouder zijn dan drie maanden worden automatisch verwijderd, tenzij er bijzondere redenen zijn om deze gegevens niet te verwijderen. Een bijzondere reden is bijvoorbeeld een zwaarwegend vermoeden van onrechtmatig gebruik dan wel misbruik van de elektronische communicatiemiddelen. Dit moet dan worden gemeld bij het CBP.
2. Indien de systeembeheerder om technische redenen persoonsgegevens, gerelateerd aan de communicatiemiddelen en het toegangspassensysteem, niet kan verwijderen, wordt onder verwijderen verstaan het niet meer verstrekken van deze gegevens voor de in artikel 3 lid 1 geformuleerde doeleinden.

Artikel 15 Personen aan wie persoonsgegevens worden verstrekt

1. De door de gemeente vastgelegde persoonsgegevens worden verstrekt aan:
 - a. Het bevoegd gezag indien er een redelijk vermoeden bestaat van onrechtmatig gebruik dan wel misbruik van de communicatiemiddelen en/of het toegangspassensysteem.
 - b. Degene die, op verzoek van het bevoegd gezag, is belast met of leiding geeft aan een onderzoek naar onrechtmatig gebruik dan wel misbruik van de communicatiemiddelen en/of het toegangspassensysteem.

HOOFDSTUK 5 RECHTEN VAN BETROKKE NE: INZAGE, VERBETEREN, AANVULLEN, VERWIJDEREN, OF AFSCHERMEN PERSOONS GEGEVENS

Artikel 16 Rechten van betrokkene

1. Aan de medewerker die daarom aan de verantwoordelijke verzoekt, wordt schriftelijk een overzicht verschaft van de hem/haar betreffende persoonsgegevens die worden verwerkt.
2. De verantwoordelijke beslist binnen vier weken na ontvangst van het in het eerste lid vernoemde verzoek. Indien een gewichtig belang van de verzoeker dit eist, voldoet de verantwoordelijke aan dit verzoek in een andere dan schriftelijke vorm, die aan dat belang is aangepast.
3. De medewerker kan de verantwoordelijke 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.
4. De verantwoordelijke bericht de verzoeker binnen vier weken na ontvangst van het in het tweede lid genoemde verzoek schriftelijk of, dan wel in hoeverre hij daaraan voldoet. Een weigering wordt gemotiveerd door de verantwoordelijke. Een beslissing op een verzoek geldt als een besluit in de zin van artikel 1:3 Algemene Wet Bestuursrecht.

5. De verantwoordelijke draagt er zorg voor dat een beslissing tot verbetering, aanvulling, verwijdering of afscherming zo spoedig mogelijk wordt uitgevoerd.
6. De medewerker kan bij de verantwoordelijke verzet aantekenen tegen de verwerking van zijn persoonsgegevens in verband met bijzondere persoonlijke omstandigheden. De verantwoordelijke oordeelt binnen vier weken na ontvangst van dit verzet of dit gerechtvaardigd is. Indien de verantwoordelijke het verzet gerechtvaardigd acht, beëindigt hij terstond de verwerking.

HOOFDSTUK 6 STRAFBEPALING, ONVOORZIENE OMSTANDIGHEDEN, OPENBAARMAKING, INWERKINGTREDING, EVALUATIE EN SLOTBEPALING

Artikel 17 Strafbepaling

1. Overtreding van dit privacyprotocol kan voor medewerkers in dienst van de gemeente resulteren in disciplinaire maatregelen als bedoeld in artikel 16:1:2 jo. artikel 8:13 CAR/LAR.
2. Overtreding van dit privacyprotocol 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. herziene afspraken over de (duur en inhoud van de) samenwerking;
 - c. herziene afspraken over de te factureren arbeidsduur.

Artikel 18 Onvoorziene omstandigheden

In gevallen waarin dit privacyprotocol niet voorziet of bij twijfel omtrent de toepassing van dit protocol, beslist het College.

Artikel 19 Openbaarmaking en evaluatie

1. Dit privacyprotocol wordt verstrekt of ter beschikking gesteld aan alle medewerkers die, direct of indirect, de beschikking krijgen over de communicatiemiddelen en/of een toegangspas.
2. Over de uitvoering van dit privacyprotocol wordt jaarlijks, aan het eind van elk kalenderjaar, geëvalueerd in opdracht van het college en gerapporteerd aan het AMT en de OR.
3. Voor de uitvoering, de evaluatie en de rapportage is het hoofd Concerncontrol verantwoordelijk.

Artikel 20 Inwerkingtreding

Dit protocol treedt in werking op 1 oktober 2011.

Artikel 21 Slotbepalingen

1. Dit protocol kan worden aangehaald als: Privacyprotocol gemeente Alkmaar.
2. De verantwoordelijke kan dit protocol met instemming van de ondernemingsraad wijzigen zoals bedoeld in artikel 27 lid 1 sub k Wet op de Ondernemingsraden. Deze wijzigingen worden schriftelijk vastgelegd en voorafgaand aan de invoering aan de medewerkers bekend gemaakt.
3. Onverminderd het bepaalde in dit privacyprotocol, zal op het verwerken van persoonsgegevens de op 1 september 2001 in werking getreden Wbp van toepassing zijn.

4. Dit privacyprotocol vervangt:
 - a. Het Protocol pc-gebruik van de gemeente Alkmaar;
 - b. Het Protocol e-mail-gebruik door medewerkers van de gemeente Alkmaar;
 - c. Het Reglement e-mail- en internetgebruik;