Gemeente Hellendoorn

GEMEENTEBLAD

Officiële uitgave van de gemeente Hellendoorn

Nr. 93982

18 april 2019

Privacyreglement e-mail- en internetgebruik

Nijverdal, 24 maart 2009 Nr. 09INT00058
Het college van burgemeester en wethouders van de gemeente Hellendoorn;
Gelet op:
- het feit dat de gemeente Hellendoorn aan degenen die bij haar organisatie werkzaam zijn e-mail- en internetfaciliteiten ter beschikking stelt om met behulp daarvan hun functie uit te oefenen;
- de wenselijkheid een Privacyreglement vast te stellen waarin naast regels voor e-mail- en internetgebruik eveneens regels zijn opgenomen voor het vastleggen en monitoren van dit gebruik;
- het bepaalde in de Wet bescherming persoonsgegevens (verder te noemen: Wbp);
- de instemming met het Privacyreglement door de Ondernemingsraad van de gemeente Hellendoorn;

b e s l u i t :
vast te stellen het volgende privacyreglement e-mail- en internetgebruik

HOOFDSTUK 1 DEFINITIES, REIKWIJDTE EN DOELEINDEN

Artikel 1 Definities

In dit privacyreglement wordt verstaan onder:
1. Wbp: Wet bescherming persoonsgegevens;
2. Gemeente: de gemeente Hellendoorn;
3. Cbp: College bescherming persoonsgegevens;
4. Medewerker: degene die aan te merken is als:
   a. werknemer in dienst van de gemeente;
   b. persoon die (betaalde of niet-betaalde) werkzaamheden voor de gemeente verricht, anders dan in ambtelijk dienstverband;
5. E-mailfaciliteiten: de door of namens de gemeente aan medewerkers ter beschikking gestelde e-mailfaciliteit;
6. Internetfaciliteiten: de door of namens de gemeente aan medewerkers ter beschikking gestelde internetfaciliteiten;
7. Elektronische communicatiemiddelen: e-mail- en/of internetfaciliteiten;
8. Persoonsgegeven: elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon in de zin van de Wbp;
9. 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;
10. Verantwoordelijke: het college, zijnde het bestuursorgaan dat het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt;
11. Onrechtmatig gebruik dan wel misbruik van de elektronische communicatiemiddelen: een doen of nalaten in strijd met dit privacyreglement of andere wet- en regelgeving of een inbreuk op een recht.

Artikel 2 Reikwijdte

1. Dit privacyreglement is van toepassing op het verwerken van persoonsgegevens inzake het gebruik van elektronische communicatiemiddelen. Dit privacyreglement geeft de wijze aan waarop in de gemeente wordt omgegaan met elektronische communicatiemiddelen en omvat regels ten aanzien van verantwoord gebruik hiervan en regels over de wijze waarop controle hiervan plaatsvindt.
2. Dit privacyreglement geldt voor werknemers in dienst van de gemeente en personen die (betaalde of niet-betaalde) werkzaamheden voor de gemeente verrichten, anders dan in ambtelijk dienstverband.

Artikel 3 Doeleinden

De verwerking van persoonsgegevens inzake het gebruik van de elektronische communicatiemiddelen heeft de volgende doeleinden:

a. het verkrijgen van inzicht in de mate van gebruik van de elektronische communicatiemiddelen;
b. het voorkomen van onrechtmatig gebruik dan wel misbruik van de elektronische communicatiemiddelen;
c. het beveiligen van het systeem en het netwerk.

HOOFDSTUK 2 VERANTWOORDELIJKHEDEN EN BEHEER

Artikel 4 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. 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.
3. Door de verantwoordelijke worden één of meerdere systeembeheerders aangewezen die belast zijn met het beheer van het (de) bestand(en). Deze systeembeheerders 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.

HOOFDSTUK 3 GEBRUIK ELEKTRONISCHE COMMUNICATIEMIDDELEN

Artikel 5 Gebruik elektronische communicatiemiddelen

1. Medewerkers gebruiken de elektronische communicatiemiddelen primair voor het uitvoeren van de hen door de gemeente opgedragen taken.
2. Incidenteel privé-gebruik van de elektronische communicatiemiddelen door medewerkers is toegestaan mits dit gebruik in overeenstemming is met dit privacyreglement 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.
3. Het is medewerkers 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 medewerkers toegestaan met behulp van de e-mailfaciliteiten illegale software te verzenden of op te vragen dan wel bestanden zonder voorafgaand overleg met de systeembeheerder(s) te verzenden of op te vragen waarvan medewerker redelijkerwijs moet aannemen dat deze te omvangrijk zijn.
4. Het is medewerkers niet toegestaan met behulp van de 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, online te gokken, illegale software te downloaden dan wel zonder voorafgaand overleg met de systeembeheerder(s) bestanden te downloaden waarvan medewerker redelijkerwijs moet aannemen dat deze te omvangrijk zijn.
5. Het is medewerkers niet toegestaan met behulp van de internetfaciliteiten persoonlijke zakelijke en/of financiële transacties te verrichten.
6. Het is medewerkers niet toegestaan videobestanden, audiobestanden of filmbanden zonder voorafgaand overleg met de systeembeheerder te verzenden, ontvangen of downloaden.
7. Streaming van audio- of videobestanden zonder voorafgaand overleg met de systeembeheerder is medewerkers niet toegestaan.
8. Het is medewerkers niet toegestaan zonder voorafgaand overleg programmatuur zelfstandig te installeren.
9. Indien medewerkers met gebruik van de internetfaciliteiten handelingen verrichten die als e-mailtoepassingen zijn te kwalificeren, dan is het derde lid van overeenkomstige toepassing.
10. Medewerkers zullen bij het gebruik van de elektronische communicatiemiddelen de nodige zorgvuldigheid betrachten en de integriteit en goede naam van de gemeente waarborgen.

HOOFDSTUK 4 CONTROLE, BEWARING EN VERWIJDERING PERSOONSGEGEVENS

Artikel 6 Controle

1. Controle door de verantwoordelijke op het gebruik van de elektronische communicatiemiddelen vindt slechts plaats in het kader van de in artikel 3 genoemde doeleinden. Deze doeleinden stellen beperkingen aan de omvang en wijze van controle.

2. Controle ter verkrijging van inzicht in de mate van gebruik van e-mail wordt beperkt tot de verkeersgegevens (tijd, hoeveelheid, omvang en dergelijke). Ter verkrijging van inzicht in de meest bezochte internetsites wordt een top tien van meest bezochte internetsites samengesteld.
3. 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. Bovendien vindt de controle in beginsel geanonimiseerd plaats.
4. 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.
5. Controle vindt in beginsel plaats door middel van 'electronic monitoring' 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. De medewerker of groep medewerkers wordt vooraf op de hoogte gebracht van de gerichte controle.
6. Controle beperkt zich in principe tot verkeersgegevens van het gebruik van de elektronische communicatiemiddelen. Alleen bij zwaarwegende redenen vindt er controle op de inhoud plaats.
7. Onrechtmatig gebruik dan wel misbruik van de elektronische communicatiemiddelen wordt zo veel mogelijk softwarematig onmogelijk gemaakt.
8. Indien geconstateerd wordt dat een medewerker dit privacyreglement overtreedt, dan wordt de betrokken medewerker zo spoedig mogelijk hierop aangesproken door de leidinggevende.
9. Het gebruik van de elektronische communicatiemiddelen door OR-leden, GO-leden, bedrijfsartsen en andere medewerkers met een vertrouwensfunctie is in beginsel uitgesloten van controle. Dit geldt niet voor de controle op de veiligheid van het elektronische verkeer.

Artikel 7 Bewaring en verwijdering

1. Persoonsgegevens, gerelateerd aan de elektronische communicatiemiddelen, worden maximaal zes maanden bewaard. 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 van de elektronische communicatiemiddelen, om de gegevens langer te bewaren. Dat moet dan expliciet kunnen worden gemaakt en worden gemeld aan het Cbp.
2. Indien de systeembeheerder om technische redenen persoonsgegevens, gerelateerd aan de elektronische communicatiemiddelen, niet kan verwijderen, wordt onder verwijderen verstaan het niet meer verstrekken van deze gegevens voor de in artikel 3 geformuleerde doeleinden.

HOOFDSTUK 5 RECHTEN VAN MEDEWERKER: VERBETEREN, AANVULLEN, VERWIJDEREN OF AFSCHERMEN PERSOONSGEGEVENS

Artikel 8 Rechten van de medewerker

1. Aan de medewerker, die daarom aan verantwoordelijke verzoekt, wordt een overzicht verschaft van de hem betreffende persoonsgegevens die worden verwerkt.
2. 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.
3. 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 is met redenen omkleed.
4. De verantwoordelijke draagt er zorg voor dat een beslissing tot verbetering, aanvulling, verwijdering of afscherming zo spoedig mogelijk wordt uitgevoerd.

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

Artikel 9 Sancties

1. Overtreding van dit privacyreglement kan voor werknemers in dienst van de gemeente resulteren in disciplinaire maatregelen of ontslag als disciplinaire straf als bedoeld in de CAR/UWO van de gemeente Hellendoorn.
2. Overtreding van dit privacyreglement kan voor personen die (betaalde of niet-betaalde) werkzaamheden voor de gemeente verrichten, anders dan in ambtelijk dienstverband, resulteren

in maatregelen waardoor deze personen, al dan niet tijdelijk, geen beschikking meer hebben over (een deel van) de elektronische communicatiemiddelen.
3. Bij strafbare feiten zal de verantwoordelijke aangifte doen bij de politie.

Artikel 10 Onvoorziene omstandigheden
In gevallen waarin dit privacyreglement niet voorziet of bij twijfel omtrent de toepassing van dit privacyreglement, beslist de verantwoordelijke.

Artikel 11 Openbaarmaking, inwerkingtreding en evaluatie
1. Dit privacyreglement wordt verstrekt of ter beschikking gesteld aan alle medewerkers die, direct of indirect, de beschikking krijgen over elektronische communicatiemiddelen.
2. Dit privacyreglement treedt in werking op 2 april 2009.
3. Dit privacyreglement wordt tweejaarlijks geëvalueerd door de verantwoordelijke en de ondernemingsraad.

Artikel 12 Slotbepaling
Onverminderd het bepaalde in dit privacyreglement, is op het verwerken van persoonsgegevens de op 1 september 2001 in werking getreden Wbp van toepassing.

Burgemeester en Wethouders van Hellendoorn,
de secretaris de burgemeester

TOELICHTING

ALGEMEEN
Instemming ondernemingsraad
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 lid 1 onder k en l Wet op de ondernemingsraden de instemming van de ondernemingsraad vereist. De ondernemingsraad dient instemming te verlenen aan de controle.

College bescherming persoonsgegevens – Vrijstellingsbesluit
Een verantwoordelijke is verplicht om de verwerking van persoonsgegevens te melden bij het College bescherming persoonsgegevens (Cbp) voordat hij begint met de verwerking. Op basis van het Vrijstellingsbesluit is het mogelijk vrijstelling van de meldingsverplichting te verkrijgen. Controle op het gebruik van e-mail en internet valt onder de vrijstelling mits voldaan wordt aan de vereisten van het Vrijstellingsbesluit, te weten, geen andere gegevens worden verwerkt dan:
a. gegevens ten behoeve van identificatie van en communicatie (username en toegangscode) met de gebruikers binnen het netwerk;
b. gegevens met betrekking tot bevoegdheden van de gebruikers en netwerkbeheerders met het oog op de aangeboden faciliteiten en diensten van het netwerk;
c. gegevens met betrekking tot de verrichtingen van de gebruikers en netwerkbeheerders, en
d. gegevens met betrekking tot elektronische berichten van of voor gebruikers.

Daarnaast geldt dat persoonsgegevens slechts worden verstrekt aan degenen, die belast zijn met de interne controle en beveiliging, met dien verstande dat verstrekking aan derden slechts geschiedt met het oog op het behandelen van geschillen.
Persoonsgegevens dienen uiterlijk zes maanden nadat ze zijn verkregen te worden verwijderd, dan wel twee jaar nadat het dienstverband of de werkzaamheden van betrokkenen ten behoeve van de verantwoordelijke zijn beëindigd.

ARTIKELSGEWIJZE TOELICHTING

Artikel 1
De Wbp is van toepassing als sprake is van verwerking van persoonsgegevens. Gegevens met betrekking tot het e-mail- en internetgebruik van medewerkers 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 medewerker. 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 medewerker de regels in het privacyreglement nakomt.
De Wbp hanteert een ruime definitie voor het begrip ‘verwerking’: het gehele proces van verzamelen tot aan vernietigen van gegevens.

Artikel 2 Reikwijdte
Het privacyreglement is van toepassing op het verwerken van persoonsgegevens inzake het gebruik van e-mail- en/of internetfaciliteiten van de gemeente.
Het privacyreglement geldt voor alle medewerkers van de gemeente: ambtenaren en personen die (betaald of niet-betaald) werkzaamheden verrichten, anders dan in ambtelijk dienstverband.
Het privacyreglement is niet van toepassing op politieke ambtsdragers.

Artikel 3 Doeleinden
De Wbp bepaalt in artikel 6 dat gegevens in overeenstemming met de wet en op een behoorlijke en zorgvuldige wijze moeten worden verwerkt.
Persoonsgegevens mogen slechts voor welbepaalde, duidelijk omschreven en gerechtvaardigde doeleinden worden verwerkt. De doelomschrijving moet nauwkeurig en zo volledig mogelijk zijn.
Als grondslag van de controle kan doorgaans het gerechtvaardigd belang van de organisatie worden aangewezen. De privacybelangen van de medewerkers horen hierbij dan wel meegewogen te worden.
De aard, omvang en vorm van de controlemaatregelen dienen in een redelijke verhouding tot het doel van de controle te staan (proportionaliteit). Tevens geldt dat de controlemiddelen niet meer inbreuk mogen maken op de belangen van de medewerker dan strikt noodzakelijk is (subsidiariteit).

Artikel 4
Lid 1
De verantwoordelijke is verplicht de gegevens zo juist en nauwkeurig mogelijk te verwerken. Dit is geen absolute verplichting. Een garantie voor de juistheid van gegevens kan van de werkgever niet worden gevergd. De redelijkheid stelt daarbij grenzen aan de te nemen maatregelen.
Lid 2
De technische en organisatorische 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.
Lid 3
De systeembeheerder is met het beheer van de bestanden belast. De systeembeheerder heeft uit hoofde van zijn functie toegang tot alle gegevens in het computernetwerk. De functie van systeembeheerder dient met de nodige waarborgen te worden omgeven. De systeembeheerder is zich ervan bewust dat hij de gegevens die hij tijdens zijn werk tegenkomt, geheim dient te houden, tenzij enige wettelijk voorschrift hem tot mededeling verplicht of uit zijn taak de noodzaak tot mededeling voortvloeit.
De systeembeheerder is in beginsel niet bevoegd tot het lezen van documenten of e-mail of het meekijken met het internetgebruik van de medewerkers zonder dat daar een bijzondere aanleiding voor is.
De systeembeheerder heeft tegenover het management een zekere onafhankelijkheid.
In het kader van de zorgvuldigheid worden regelmatig back-ups gemaakt. Van deze back-ups mag niet onzorgvuldig of onbevoegd gebruik gemaakt worden. Back-ups dienen dan ook op een veilige plaats bewaard te worden. Nadat gegevens zijn aangepast moet zo snel mogelijk een nieuwe back-up gemaakt worden en moeten oude versies worden vernietigd, zodat de gegevens niet na een eventuele terugplaatsing van een back-up nogmaals moeten worden aangepast.

Artikel 5
In dit artikel zijn gedragsregels opgenomen wat onder verantwoord e-mail- en internetgebruik wordt verstaan.
Een totaalverbod op het privé-gebruik van elektronische communicatiemiddelen is niet mogelijk. Er is een uitspraak gedaan over privatisering van de werkplek. Een bepaalde mate van niet-zakelijk e-mail- en internetgebruik onder werktijd kan niet worden verboden (Kanton Haarlem, 16-06-2000). De werkgever kan wel beperkende voorwaarden verbinden aan het persoonlijk gebruik van de elektronische communicatiemiddelen.

Artikel 6
Lid 1
Controle vindt plaats door de verantwoordelijke in het kader van de in artikel 3 genoemde doeleinden.
Ten aanzien van het eerste doeleinde, het verkrijgen van inzicht in de mate van gebruik van de elektronische communicatiemiddelen voert de systeembeheerder de controle uit onder verantwoordelijkheid van het college.
Ten aanzien van het tweede doeleinde, het voorkomen van onrechtmatig gebruik dan wel misbruik van de elektronische communicatiemiddelen, signaleert de systeembeheerder en bepaalt de clustermanager het vervolgtraject.
Controle ten aanzien van het derde doeleinde, het beveiligen van het systeem en het netwerk, vindt plaats door de systeembeheerder onder verantwoordelijkheid van het college.
Lid 2

In het kader van kosten- en capaciteitsbeheersing blijft de controle ter verkrijging van inzicht in de mate van het gebruik van e-mail beperkt tot de verkeersgegevens (zoals tijd, hoeveelheid, omvang, etc.). Ter verkrijging van inzicht in de meest bezochte internetsites wordt een top tien vastgesteld. Daarvoor wordt wel kennisgenomen van inhoudelijke gegevens.
Lid 3
Controle ter voorkoming van onrechtmatig gebruik dan wel misbruik wordt zo beperkt mogelijk gehouden. De genomen maatregelen moeten in redelijke verhouding staan tot de belangen van de medewerker en de gebruikte middelen mogen niet een verdergaande inbreuk maken op die belangen dan strikt noodzakelijk (proportionaliteit, subsidiariteit).
Een belangenafweging dient telkenmale plaats te vinden. Het doel rechtvaardigt niet een continue controle en de daarmee gepaard gaande verregaande inbreuk op de persoonlijke levenssfeer van de werknemer. Controle op de naleving mag in beginsel slechts steekproefsgewijs geschieden.
Lid 4
Vanuit beveiligingsoogpunt is het wenselijk om e-mail- en internetgebruik te controleren. Het gaat dan om het tegengaan van onder andere systeemaanvallen van virussen, trojans of andere schadelijke programma's.
Deze controle vindt zowel voor e-mail- als voor internetgebruik geheel geautomatiseerd plaats. Wanneer een besmet bericht wordt gevonden, wordt dit op een aparte locatie bewaard voor nader onderzoek en eventueel herstelwerkzaamheden.
Lid 5
Controle vindt in beginsel plaats op het niveau van getotaliseerde gegevens die niet herleidbaar zijn tot individuele personen. Wanneer een medewerker of een groep medewerkers wordt verdacht van het overtreden van de regels, vindt gedurende een periode van vier weken een aangekondigde gerichte controle plaats.
De gegevens in de managementrapportages en gebruiksstatistieken van het e-mail- en internetgebruik worden ontdaan van hun identificerende kenmerken. Slechts bij concrete bedenkingen tegen een bepaalde medewerker is een rapportage op persoonsniveau noodzakelijk en toegestaan.
Lid 7
Onrechtmatig gebruik dan wel misbruik van de elektronische communicatiemiddelen is ingebouwd in de software die wordt gebruikt om te e-mailen en internetten.
Lid 8
Wanneer geconstateerd wordt dat een medewerker het privacyreglement overtreedt, dan wordt de betrokken medewerker zo spoedig mogelijk hierop aangesproken door de leidinggevende. De direct leidinggevende draagt hiervoor zorg.
Wanneer de medewerker op zijn handelen in strijd met het privacyreglement wordt aangesproken, wordt hij gewaarschuwd voor de (rechtspositionele) gevolgen bij continuering van dit gedrag.
Lid 9
Communicatie via e-mail van leden van de ondernemingsraad en het georganiseerd overleg (GO) ten behoeve van hun ondernemingsraad (GO)-werkzaamheden valt buiten de controle. Op grond van artikel 17 Wet op de ondernemingsraden hebben leden van de ondernemingsraad (en het GO) het recht om onderling te overleggen met gebruik van voorzieningen waarover het lid als zodanig kan beschikken. Er is geen sprake van een gezagsrelatie. De werkgever kan de gezagsbevoegdheid dan ook niet aanwenden om het e-mailgebruik van leden van de ondernemingsraad en het GO in functie te controleren.

Artikel 7
De standaardtermijn voor het bewaren van persoonsgegevens bedraagt zes maanden. In het geval van een zwaarwegend vermoeden van onrechtmatig gebruik dan wel misbruik van elektronische communicatiemiddelen, worden de gegevens uit die zes maanden bewaard, zolang dit in het kader van nader onderzoek en eventueel te treffen maatregelen jegens een medewerker noodzakelijk is. Zodra een nader onderzoek is afgerond en niet leidt tot maatregelen jegens een medewerker worden de gegevens verwijderd.
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 het Nederlands culturele erfgoed.
Bepaalde gegevens kunnen om technische redenen niet worden verwijderd. Via 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 verwerkt (verstrekt).

Artikel 8
Transparantie is een belangrijk beginsel voor privacybescherming. De informatieplicht is gebaseerd op de artikelen 33 en 34 Wbp.

Artikel 9

Bij overtreding van het privacyreglement kunnen disciplinaire maatregelen of ontslag of ontslag als disciplinaire maatregel worden opgelegd.
Tegen het opleggen van disciplinaire maatregelen en straffen kan op basis van de Algemene wet bestuursrecht bezwaar en beroep worden aangetekend.

Artikel 11
Het privacyreglement moet helder naar de medewerkers worden gecommuniceerd. De medewerkers moeten weten wat verboden is en wat is toegestaan, dat controle mogelijk is, op welke manier de controle geschiedt en wat de consequenties zijn bij overtreding van het privacyreglement.