

MODELGEDRAGSCODE INTERNET EN E-MAILGEBRUIK

De XYZ BV, gevestigd te Amsterdam

Gelet op

Artikel 7:611 en 7:660 van het Burgerlijk Wetboek
Algemene Verordening Gegevensbescherming (AVG)

Artikel 27 lid 1 sub k en l Wet op de Ondernemingsraden

Overwegende dat

De XYZ BV en haar werknemers zich ten opzichte van elkaar dienen te gedragen als een goed werkgever en een goed werknemer (art. 7:611 BW).

Het gebruik van internet en e-mailgebruik voor (veel van) de werknemers binnen XYZ BV noodzakelijk is om hun werk goed te kunnen doen.

Aan het gebruik van internet risico's verbonden zijn die nopen tot het stellen van gedragsregels.

Tegen de achtergrond van deze risico's van de werknemers verantwoord gebruik van internet en e-mail wordt verwacht.

XYZ BV gerechtigd is tot het geven van voorschriften voor gebruik van internet en e-mail en het nemen van maatregelen ter bevordering van de goede orde in de onderneming (artikel 7:660 BW)

De onderhavige gedragscode voorschriften en maatregelen bevat zoals hiervoor genoemd.

XYZ BV gerechtigd is persoonsgegevens te verwerken ten behoeve van de controle op de naleving van deze gedragscode

XYZ BV bij de controle de fundamentele rechten en vrijheden van de betrokken werknemer(s) in acht neemt, in het bijzonder het recht op bescherming van de persoonlijke levenssfeer (artikel 8 sub f WBP)

heeft (...met instemming van de ondernemingsraad..) de volgende gedragscode vastgesteld.

Gedragscode internet en e-mail gebruik

1 Werkingsfeer

Deze regeling is van toepassing op alle geheel of gedeeltelijk geautomatiseerde verwerkingen van persoonsgegevens van personen in dienst van of werkzaam voor XYZ BV.

2 Uitgangspunten

- 2.1 De controle op persoonsgegevens over e-mail en internetgebruik is een verwerking van persoonsgegevens in de zin van de Algemene Verordening Gegevensbescherming (AVG)
- 2.2 De controle op e-mail- en internetgebruik binnen XYZ BV zal conform deze regeling worden uitgevoerd. Indien er zich situaties voordoen waarin deze regeling niet voorziet, zal conform het arbeidsrechtelijk kader en de WBP en in overleg met de ondernemingsraad gehandeld worden.
- 2.3 Gestreefd wordt naar een goede balans tussen verantwoord e-mail en internetgebruik en bescherming van de privacy van werknemers op de werkplek.
- 2.4 Persoonsgegevens over e-mail en internetgebruik worden niet langer bewaard dan noodzakelijk, met een maximum bewaartermijn van 6 maanden.
- 2.5 De werkgever treft voorzieningen over de positie en integriteit van de systeembeheerder en/of afdeling systeembeheer en de controle daarop.

3 Doel

- 3.1 Deze gedragscode bevat regels ten aanzien van verantwoord e-mail en internetgebruik en regels over de wijze waarop controle op persoonsgegevens over e-mail- en internetgebruik plaats vindt.

De controle op persoonsgegevens over e-mail en internetgebruik vindt plaats met als doel

- 3.2
- a. Begeleiding/individuele beoordeling
 - b. Voorkomen van negatieve publiciteit
 - c. Tegengaan van seksuele intimidatie
 - d. Controle op bedrijfsgeheimen
 - e. Systeem en netwerkbeveiliging
 - f. Kosten en capaciteitsbeheersing
 - g. Tegengaan van discriminatie

4 E-mailgebruik

- 4.1 Het e-mail systeem wordt aan de werknemer voor zakelijk gebruik beschikbaar gesteld. Gebruik is derhalve verbonden met taken die voortvloeien uit de functie.
- 4.2 Beperkt persoonlijk gebruik van het e-mailsysteem is evenwel toegestaan, mits dit niet storend is voor de dagelijkse werkzaamheden en dit geen verboden gebruik in de zin van artikel 5 oplevert.
- 4.3 Werknemers mogen het e-mailsysteem gebruiken voor het ontvangen en versturen van e-mailberichten mits dit beperkt blijft tot 30 minuten per dag.

4.4 Werknemers mogen het e-mailsysteem gebruiken voor het ontvangen en versturen van persoonlijke e-mailberichten mits dit niet storend is voor de dagelijkse werkzaamheden en het computernetwerk

4.5 Werknemers mogen incidenteel en kortstondig het e-mailsysteem gebruiken voor het ontvangen en versturen van persoonlijke e-mailberichten mits dit niet storend is voor de dagelijkse werkzaamheden en het computernetwerk

5 Verboden e-mailgebruik

5.1 Het is de werknemer niet toegestaan om het e-mail systeem te gebruiken voor het verzenden van berichten met een pornografische, racistische, discriminerende, beledigende of aanstootgevende inhoud.

5.2 Het is de werknemer niet toegestaan om het e-mail systeem te gebruiken voor het verzenden van berichten met een (seksueel) intimiderende inhoud.

5.3 Het is de werknemer niet toegestaan om het e-mail systeem te gebruiken voor het verzenden van berichten die (kunnen) aanzetten tot haat en/of geweld.

5.4 Het is de werknemer niet toegestaan om het e-mail systeem te gebruiken voor het versturen en ontvangen van kettingbrieven.

5.5 Het is de werknemer niet toegestaan om het e-mail systeem te gebruiken voor het versturen van e-mailberichten met een dreigende inhoud

6 Internetgebruik

6.1 Internetsysteem wordt aan de werknemer voor zakelijk gebruik beschikbaar gesteld. Gebruik is derhalve verbonden met taken die voortvloeien uit de functie.

6.2 Beperkt persoonlijk gebruik van het internetgebruik is evenwel toegestaan, mits dit niet storend is voor de dagelijkse werkzaamheden en dit geen verboden gebruik in de zin van artikel 7 oplevert.

6.3 Voor het gebruik van het internetsysteem voor persoonlijke doeleinden stelt de organisatie een aparte computer beschikbaar, die zich werkplek kantoor Amsterdam bevindt. Het is niet toegestaan om de computer op de eigen werkplek hiervoor te gebruiken.

6.4 Werknemers mogen het internetsysteem voor persoonlijke doeleinden gebruiken, mits dit beperkt blijft tot 60 minuten per dag .

6.5 Werknemers mogen het internetsysteem voor persoonlijke doeleinden gebruiken, mits dit niet storend is voor de dagelijkse werkzaamheden en het computernetwerk.

6.6 Werknemers mogen incidenteel en kortstondig het internetsysteem voor persoonlijke doeleinden gebruiken, mits dit niet storend is voor de dagelijkse werkzaamheden en het computernetwerk.

7 Verboden internetgebruik

7.1 Het is de werknemer niet toegestaan om op internet sites te bezoeken die pornografisch, racistisch, discriminerend, beledigend of aanstootgevend materiaal bevatten. Noch is het toegestaan dergelijk materiaal te downloaden

7.2 Het is de werknemer niet toegestaan om zich ongeoorloofd toegang tot niet openbare bronnen op internet te verschaffen.

7.3 Het is de werknemer niet toegestaan om op internet in strijd met de wet of onethisch handelen.

7.4 Het is de werknemer niet toegestaan om software en applicaties te downloaden.

8 Voorwaarden voor controle

- 8.1 Controle van persoonsgegevens over e-mail en internetgebruik vindt slechts plaats in het kader van in artikel 3.2 genoemde doelen.
- 8.2 Controle vindt in beginsel plaats op het niveau van getotaliseerde gegevens die niet herleidbaar zijn tot identificeerbare persoon.
- 8.3 Indien een werknemer of een groep werknemers wordt verdacht de regels te overtreden, kan gedurende een vastgestelde (korte) periode gerichte controle plaatsvinden.
- 8.4 Controle beperkt zich in beginsel tot verkeersgegevens van het e-mail en internetgebruik slechts bij zwaarwegende redenen vindt controle op de inhoud plaats.
- 8.5 Verboden e-mail en internetgebruik wordt zo veel mogelijk softwarematig onmogelijk gemaakt. Overige controle vindt slechts steekproefsgewijs plaats.
- 8.6 Bij constatering van verboden gebruik wordt dit onmiddellijk met de betrokken werknemer besproken. De werknemer wordt gewezen op de consequenties wanneer hij niet stopt met het verboden gebruik.
- 8.7 E-mail berichten van leden van de ondernemingsraad onderling, van bedrijfsartsen en van een ieder die zich op grond van zijn functie op enige vertrouwelijkheid moet kunnen beroepen worden niet gecontroleerd.

9 Controle

- 9.1 De controle in het kader van begeleiding en/of individuele beoordeling vindt steekproefsgewijs plaats en beperkt zich tot zakelijke mailberichten.
- 9.2 De controle ter voorkoming van negatieve publiciteit en seksuele intimidatie en de controle in het kader van systeem- en netwerkbeveiliging vindt plaats op basis van content-filtering. Verdachte berichten worden automatisch teruggestuurd naar de afzender.
- 9.3 De controle op het uitlekken van bedrijfsgeheimen vindt plaats op basis van steekproefsgewijze content-filtering. Verdachte berichten worden apart gezet voor nader onderzoek.
- 9.4 De controle in het kader van kosten- en capaciteitsbeheersing wordt beperkt tot verkeersgegevens.

10 Rechten van de werknemer

10.1 XYZ BV informeert de werknemer voorafgaand aan de controle op persoonsgegevens over e-mail en internetgebruik, omtrent de doeleinden, de aard van de gegevens, de omstandigheden waaronder zij verkregen zijn en de inhoud van deze regeling.

10.2 De werknemer kan zich tot XYZ BV wenden met het verzoek voor een volledig overzicht van zijn bewerkte persoonsgegevens. Het verzoek wordt binnen 4 weken beantwoord.

10.3 De werknemer kan de XYZ BV verzoeken zijn persoonsgegevens te verbeteren, aan te vullen, te verwijderen of af te schermen indien deze feitelijk onjuist zijn, voor het doel onvolledig of niet ter zake dienend zijn, dan wel in strijd met een wettelijk voorschrift zijn. Het verzoek wordt binnen 4 weken beantwoord.

11 Slotbepaling

XYZ BV kan deze gedragscode met instemming van de ondernemingsraad wijzigen of intrekken.

Toelichting

Algemeen

De invoering van een gedragscode voor het gebruik van e-mail en internet is een besluit waarvoor de instemming van de ondernemingsraad nodig is (artikel 27 lid 1 sub l WOR). De hier gepresenteerde modelgedragscode is een handreiking welke aan de specifieke situatie binnen een onderneming kan worden aangepast. In deze toelichting treft men ook andere voorbeelden van verboden e-mail en internetgebruik en andere voorbeelden van verantwoord gebruik van het e-mail en internetsysteem. Zie hiervoor de toelichting bij de artikelen 4 t/m 7. Afhankelijke van de organisatie, werkzaamheden of bedrijfsrisico, kan gebruik van het e-mail en internetsysteem worden in meer of mindere mate worden beperkt. Hierbij is het uiteraard van belang dat tevoren bekend is wat wel en wat niet is toegestaan. Wanneer de werkgever een controlemaatregel wil invoeren dient hij tevoren het doel voor de controlemaatregel bekend te maken. Voorbeelden (niet limitatief!) hiervoor zijn genoemd in artikel 3 van de Gedragscode.

Artikel 1

Deze gedragscode is van toepassing op (geheel of gedeeltelijke) geautomatiseerde verwerking van persoonsgegevens van personen in dienst van of werkzaam voor de onderneming. Hier vallen niet alleen de personen onder, die een arbeidsovereenkomst hebben met de onderneming, maar ook de personen die bij de onderneming zijn gedetacheerd, uitzendkrachten, stagiaires, vrijwilligers etc.

Artikel 2

De hoofdregel van de Algemene Verordening Gegevensbescherming (AVG) eist dat persoonsgegevens op behoorlijke en zorgvuldige wijze en in overeenstemming met de wet worden verwerkt. De WBP kent een ruime betekenis toe aan het begrip 'verwerking van persoonsgegevens'. Hieronder wordt verstaan 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 terbeschikking stelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens. Een persoonsgegeven in de zin van de WBP is elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon. Het kan om allerlei soorten informatie gaan: om eigenschappen van de betrokkene, diens opvattingen of gedragingen. Meer in het algemeen gaat het om gegevens die bepalend kunnen zijn voor de manier waarop de betrokken persoon in het maatschappelijk verkeer wordt beoordeeld of behandeld.

Artikel 3

Persoonsgegevens mogen slechts voor bepaalde en gerechtvaardigde doeleinden worden verzameld en niet worden verwerkt voor doeleinden die daarmee onverenigbaar zijn. De werkgever (verantwoordelijke) moet de doelen bepalen vóórdat hij begint met het verwerken van persoonsgegevens. Hierbij is van belang dat het doel van de verwerking zo nauwkeurig en volledig mogelijk wordt omschreven. Als er meerdere doelstellingen zijn moeten deze afzonderlijk worden genoemd en getoetst op de noodzaak om met het oog hierop persoonsgegevens te verzamelen. In overleg met de ondernemingsraad moet worden vastgesteld welke doeleinden voor controle van e-mail en internetgebruik noodzakelijk zijn voor de eigen organisatie. De privacybelangen van de werknemers horen hierbij meegewogen te worden.

De doeleinden, die in artikel 3.2 worden genoemd, zijn voorbeelden van de meest voorkomende doeleinden voor controle op e-mail en internetgebruik. De hier genoemde voorbeelden zijn uiteraard niet limitatief.

a. begeleiding en individuele beoordeling

In het kader van begeleiding of individuele beoordeling van werknemers kan controle op de inhoud van de zakelijke e-mail aan de orde zijn. Deze controle moet verband houden met de taken van de werknemer. Indien een medewerker (mede) tot taak heeft per e-mail met klanten te communiceren, kan hij aan een steekproefsgewijze inhoudelijke controle onderworpen worden. De controle uitgevoerd in het kader van deze doelstelling dient zich uitsluitend te richten op zakelijke e-mail en mag niet structureel van aard zijn. Indien de werkgever geen bezwaren heeft tegen het gebruik van het e-mailsysteem voor privé-doeleinden, is het vanuit het oogpunt van bescherming van de persoonlijke levenssfeer van de werknemers wenselijk de zakelijke mail van de privé-mail te scheiden. Indien scheiding tussen zakelijke en privé-mail onmogelijk blijkt dient de werkgever de privé-mail zoveel mogelijk te ontzien.

b. Voorkomen van negatieve publiciteit

Werknemers kunnen via e-mail de goede naam van een organisatie behoorlijk aantasten. Het plegen van strafbare feiten, seksuele intimidatie of discriminerende uitingen geschiedt immers onder gebruikmaking van het e-mailadres van de organisatie. Het verdient de voorkeur hier de controle geheel geautomatiseerd te laten plaatsvinden middels content-filtering. Verdachte berichten – zowel inkomende als uitgaande – dienen zoveel mogelijk (geautomatiseerd) te worden teruggestuurd naar de afzender, waardoor vastlegging van de inhoud van het bericht niet nodig is. Bij gebruik van het internetverkeer via vaste IP-adressen kan een bezoek aan een bepaalde internet-site altijd herleid worden tot een bepaalde organisatie. Om negatieve publiciteit te voorkomen, kan de werkgever het internetgebruik steekproefsgewijs controleren, mits deze doelstellingen reeds van te voren is vastgelegd en in de onderneming bekend is gemaakt.

c. Tegengaan van seksuele intimidatie

Via e-mail kan eenvoudig seksuele intimidatie worden gepleegd. Zowel de inhoud van het bericht als de bijlagen kunnen seksueel intimiderend zijn. Een werkgever die het beleid hiervoor wil handhaven, kan inkomende berichten onderwerpen aan een geautomatiseerde controle. De tekst kan gescand worden op verboden woorden en kunnen verdachte berichten (geautomatiseerd) teruggestuurd te worden aan de oorspronkelijke afzender. Op die wijze kan de privacy van de werknemers ongeschonden blijven.

d. Controle op bedrijfsgeheimen

Controle op het uitlekken van bedrijfsgeheimen via e-mail en internet zal zoveel mogelijk moeten geschieden via geautomatiseerde controle middels content-filtering.

e. Systeem en netwerkbeveiliging

Vanuit beveiligingsoogpunt is het wenselijk om e-mail te controleren. Het kan dan gaan om het tegengaan van systeemaanvallen door virussen of andere schadelijke programma's. bij deze controle verdient een geheel geautomatiseerde controle van de inkomende berichten en de bijlagen de voorkeur. Indien een besmet bericht gevonden wordt kan dit op een aparte locatie worden bewaard voor nader onderzoek en eventuele herstelwerkzaamheden.

f. Kosten en capaciteitsbeheersing

Uiteraard kost het versturen van e-mail geld en legt het beslag op de beschikbare capaciteit van het netwerk. Het kostenaspect is met name aan de orde als de e-mailverbinding via de telefoon loopt. Deze vorm van controle kan beperkt blijven tot het controleren van de verkeersgegevens. Kennisneming van de inhoud van de mail is voor dit doel niet noodzakelijk.

g. Tegengaan van discriminatie

Zie sub c.

Artikel 4

In de gedragscode kunnen gedragsregels worden opgenomen over wat er in een organisatie onder verantwoord e-mailgebruik wordt verstaan. Een totaal verbod op het versturen en ontvangen van persoonlijke e-mailberichten is niet mogelijk. De organisatie kan wel beperkende voorwaarden stellen aan het persoonlijk gebruik van het e-mailsysteem. Hieronder treft u een aantal andere opties aan:

- Werknemers mogen het e-mailsysteem gebruiken voor het ontvangen en versturen van e-mailberichten mits dit beperkt blijft tot 30 minuten per dag.
- Werknemers mogen het e-mailsysteem gebruiken voor het ontvangen en versturen van persoonlijke e-mailberichten mits dit niet storend is voor de dagelijkse werkzaamheden en het computernetwerk
- Werknemers mogen incidenteel en kortstondig het e-mailsysteem gebruiken voor het ontvangen en versturen van persoonlijke e-mailberichten mits dit niet storend is voor de dagelijkse werkzaamheden en het computernetwerk

Artikel 5

In de gedragscode kunnen gedragsregels worden opgenomen over wat niet toegestaan is bij een verantwoord e-mailgebruik. Andere voorbeelden van verboden gebruik zijn:

- Het versturen en ontvangen van kettingbrieven
- Het versturen van e-mailberichten met een dreigende inhoud

Artikel 6

In de gedragscode kunnen gedragsregels worden opgenomen over wat er in de organisatie onder verantwoord internetgebruik wordt verstaan. Hieronder treft een aantal andere opties aan:

- Voor het gebruik van het internetsysteem voor persoonlijke doeleinden stelt de organisatie een aparte computer beschikbaar, die zich werkplek kantoor Amsterdam bevindt. Het is niet toegestaan om de computer op de eigen werkplek hiervoor te gebruiken.
- Werknemers mogen het internetsysteem voor persoonlijke doeleinden gebruiken, mits dit beperkt blijft tot 60 minuten per dag .
- Werknemers mogen het internetsysteem voor persoonlijke doeleinden gebruiken, mits dit niet storend is voor de dagelijkse werkzaamheden en het computernetwerk.
- Werknemers mogen incidenteel en kortstondig het internetsysteem voor persoonlijke doeleinden gebruiken, mits dit niet storend is voor de dagelijkse werkzaamheden en het computernetwerk.

Een totaal verbod op het internetgebruik voor persoonlijke doeleinden is niet mogelijk.

Artikel 7

In de gedragscode kunnen regels worden opgenomen over wat niet is toegestaan bij een verantwoord internetgebruik. Hieronder treft u een aantal andere opties aan:

- Op internet in strijd met de wet of onethisch handelen
- Software en applicaties downloaden
- Etc

Artikel 8

- Wanneer de werkgever constateert dat een werknemer zich schuldig maakt aan verboden gebruik van het e-mail en/of internetsysteem, bespreekt hij dit onmiddellijk met de betrokken werknemer. Daarbij wordt de werknemer gewaarschuwd voor de (rechtspositionele) consequenties die het verboden gebruik van het e-mail en/of internetsysteem voor hem kan hebben. De werkgever kan bijvoorbeeld wijzen op de risico's, zoals ontslag, die verbonden zijn aan verboden gebruik van het internet.
- 8.5 E-mailberichten van leden van de ondernemingsraad en bedrijfsartsen mogen niet worden gecontroleerd. Dit geldt eveneens voor andere in de onderneming werkzame personen die op grond van hun functie op enige vertrouwelijkheid moeten kunnen beroepen. Voorbeelden hiervan zijn leden van een personeelsvertegenwoordiging, vertrouwenspersonen, leden van een (interne) klachtencommissie etc.
- 8.6

Artikel 10

De betrokken werknemer heeft het recht zich vrijelijk en met redelijke tussenpozen tot zijn werkgever te wenden met het verzoek hem mede te delen of hem betreffende persoonsgegevens worden verwerkt. De werkgever deelt de betrokkene schriftelijk binnen vier weken mee of hem betreffende persoonsgegevens worden verwerkt. De betrokken werknemer kan de werkgever verzoeken de hem betreffende persoonsgegevens te verbeteren, aan te vullen, te verwijderen of af te schermen indien deze gegevens:

- 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 of met deze gedragscode zijn verwerkt.

De werkgever bericht de verzoeker binnen vier weken na ontvangst van het verzoek van de werknemer schriftelijk of dan wel in hoeverre hij daaraan voldoet. Een weigering is met redenen omkleed. De werkgever draagt er zorg voor dat een beslissing tot verbetering, aanvulling, verwijdering of afscherming zo spoedig mogelijk wordt uitgevoerd.