BLAD GEMEENSCHAPPELIJKE REGELING

Nr. 808

17 september 2021

Officiële uitgave van de gemeenschappelijke regeling Veiligheidsregio Zuid-Holland Zuid

# Gedragscode telefoon-, internet en e-mailgebruik Veiligheidsregio Zuid-Holland Zuid

## 1 Gedragscode telefoon, internet en e-mail gebruik

De Veiligheidsregio Zuid-Holland Zuid,

Gelet op
- Hoofdstuk 15 de CAR UWO
- De Algemene Verordening Gegevensbescherming
- Artikel 27 lid 1 sub k en l Wet op de Ondernemingsraden

Overwegende dat:

De Veiligheidsregio Zuid-Holland Zuid en haar werknemers zich ten opzichte van elkaar dienen te gedragen als een goed werkgever en een goed werknemer betaamt (artikel 15:1 CAR UWO);

Het gebruik van telefoon, e-mail en internet voor (veel van) de werknemers binnen de Veiligheidsregio Zuid-Holland Zuid noodzakelijk is om hun werk goed te kunnen uitvoeren;

Aan het gebruik risico's verbonden zijn die leiden tot het stellen van gedragsregels;

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

De Veiligheidsregio Zuid-Holland Zuid gerechtigd is tot het geven van voorschriften voor gebruik van telefoon, e-mail en internet en het nemen van maatregelen ter bevordering van de goede orde in de organisatie;

De onderhavige gedragscode voorschriften en maatregelen bevat zoals hiervoor genoemd;

De Veiligheidsregio Zuid-Holland Zuid gerechtigd is persoonsgegevens te verwerken ten behoeve van de controle op de naleving van deze gedragscode;

De Veiligheidsregio Zuid-Holland Zuid 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;

De Veiligheidsregio Zuid-Holland Zuid heeft met instemming van de ondernemingsraad, in haar vergadering van 28 november 2019, de volgende gedragscode vastgesteld.

**Gedragscode telefoon, internet en e-mail gebruik**

### Artikel 1 Werkingssfeer

Deze regeling is van toepassing op alle geheel of gedeeltelijk geautomatiseerde verwerkingen van persoonsgegevens van personen in dienst van of werkzaam voor de Veiligheidsregio Zuid-Holland Zuid.

### Artikel 2 Uitgangspunten

2.1 De controle op persoonsgegevens over telefoon-, e-mail- en internetgebruik is een verwerking van persoonsgegevens in de zin van de Algemene Verordening Gegevensbescherming.

2.2 De controle op telefoon-, e-mail- en internetgebruik binnen de Veiligheidsregio Zuid-Holland Zuid zal conform deze regeling worden uitgevoerd.

2.3 Gestreefd wordt naar een goede balans tussen verantwoord telefoon-, e-mail- en internetgebruik en bescherming van de privacy van werknemers op de werkplek.

2.4 Persoonsgegevens over telefoon-, 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.

**Artikel 3 Doel**

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

3.2 De controle op persoonsgegevens over telefoon-, e-mail en internetgebruik vindt plaats met als doel:

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

**Artikel 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 Aan het e-mailsysteem is een agenda gekoppeld. Deze agenda dient actueel te zijn en in hoofdzaak voor zakelijke doeleinden te worden gebruikt, maar kan en mag door de werknemer ook voor privédoeleinden worden gebruikt. Dit laat echter onverlet dat, voor organisatorische doeleinden, op verzoek van de leidinggevende de agenda opengesteld wordt.

4.4 Bij uitdiensttreding is werkgever gerechtigd het emailaccount van werknemer te (laten) beheren voor een periode van twee maanden. Na deze periode wordt het emailaccount gedeactiveerd.

**Artikel 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.

**Artikel 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.

**Artikel 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.

**Artikel 8 Telefoongebruik**

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

8.2 Beperkt persoonlijk gebruik van de telefoon is evenwel toegestaan, mits dit niet storend is voor de dagelijkse werkzaamheden en dit geen verboden gebruik in de zin van artikel 9 oplevert .

**Artikel 9 Verboden telefoongebruik**

9.1 Het is de werknemer niet toegestaan om de telefoon te gebruiken voor het verzenden van berichten met een pornografische, racistische, discriminerende, beledigende of aanstootgevende inhoud.

9.2 Het is de werknemer niet toegestaan om de telefoon te gebruiken voor het verzenden van berichten met een (seksueel) intimiderende inhoud.

9.3 Het is de werknemer niet toegestaan om de telefoon te gebruiken voor het verzenden van berichten die (kunnen) aanzetten tot haat en/of geweld.

### Artikel 10 Voorwaarden voor controle

10.1 Controle van persoonsgegevens over telefoon, e-mail en internetgebruik vindt slechts plaats in het kader van in artikel 3.2 genoemde doelen.
10.2 Controle vindt in beginsel plaats op het niveau van getotaliseerde gegevens die niet herleidbaar zijn tot identificeerbare persoon.
10.3 Indien een werknemer of een groep werknemers wordt verdacht de regels te overtreden, kan gedurende een vastgestelde (korte) periode gerichte controle plaatsvinden.
10.4 Controle beperkt zich in beginsel tot verkeersgegevens van het telefoon, e-mail en internetgebruik slechts bij zwaarwegende redenen vindt controle op de inhoud plaats.
10.5 Verboden telefoon, e-mail en internetgebruik wordt zo veel mogelijk softwarematig onmogelijk gemaakt. Overige controle vindt slechts steekproefsgewijs plaats.
10.6 Bij constatering van verboden gebruik wordt dit met de leidinggevende van de betrokken werknemer besproken. De leidinggevende bespreekt het geconstateerde onmiddellijk met de betrokken werknemer. De werknemer wordt gewezen op de consequenties wanneer hij niet stopt met het verboden gebruik.
10.7 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.

### Artikel 11 Controle

11.1 De controle in het kader van begeleiding en/of individuele beoordeling vindt steekproefsgewijs plaats.
11.2 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.
11.3 De controle op het uitlekken van vertrouwelijke informatie vindt plaats op basis van steekproefsgewijze content-filtering. Verdachte berichten worden apart gezet voor nader onderzoek.
11.4 De controle in het kader van kosten- en capaciteitsbeheersing wordt beperkt tot verkeersgegevens.

### Artikel 12 Rechten van de werknemer

12.1 De Veiligheidsregio Zuid-Holland Zuid informeert de werknemer voorafgaand aan de controle op persoonsgegevens over telefoon, e-mail en internetgebruik, omtrent de doeleinden, de aard van de gegevens, de omstandigheden waaronder zij verkregen zijn en de inhoud van deze regeling.
12.2 De werknemer kan zich tot de Veiligheidsregio Zuid-Holland Zuid wenden met het verzoek voor een volledig overzicht van zijn bewerkte persoonsgegevens. Het verzoek wordt binnen 4 weken beantwoord.
12.3 De werknemer kan de Veiligheidsregio Zuid-Holland Zuid 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.

### Artikel 13 Sancties

13.1 Overtreding van deze regeling kan voor medewerkers in dienst van de Veiligheidsregio Zuid-Holland Zuid resulteren in disciplinaire maatregelen als bedoeld in hoofdstuk 16 CAR-UWO.
13.2 De Veiligheidsregio Zuid-Holland Zuid is gerechtigd om eventuele schade die voor de Veiligheidsregio Zuid-Holland Zuid ontstaat door overtreding van deze regeling te verhalen op de medewerker.
13.3 Overtreding van deze regeling kan voor personen die werkzaamheden voor de Veiligheidsregio Zuid-Holland Zuid 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. Ook is de Veiligheidsregio Zuid-Holland Zuid gerechtigd om eventuele schade die voor de Veiligheidsregio Zuid-Holland Zuid ontstaat door overtreding van deze regeling op deze personen te verhalen.

### Artikel 14 Onvoorziene omstandigheden

In gevallen waarin deze regeling niet in redelijkheid voorziet beslist het Dagelijks Bestuur binnen de kaders van de CAR-UWO en de AVG.

### Artikel 15 Slotbepaling

Veiligheidsregio Zuid-Holland Zuid kan deze gedragscode met instemming van de ondernemingsraad wijzigen of intrekken.

## 2 Toelichting op de Gedragscode telefoon, internet en e-mail gebruik

**Algemeen**
De scheidingslijn tussen zakelijk en privé vervaagt steeds verder. Het is in dat licht goed te benoemen welke zakelijke communicatie middelen ook privé gebruikt kunnen en mogen worden en de wijze van controle daarop. Welke gedrag gewenst is en welk gedrag ongewenst, met de maatregelen die daarop kunnen volgen. Met de invoering van de Algemene Verordening Gegevensbescherming is nogmaals het belang van de privacy van werknemers en het verwerken van persoonsgegevens onderstreept.

De invoering van een gedragscode voor het gebruik van telefoon, e-mail en internet is een besluit waarvoor de instemming van de ondernemingsraad nodig is (artikel 27 lid 1 sub l WOR).

**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 zoals gedetacheerden, uitzendkrachten, stagiaires, vrijwilligers etc.

**Artikel 2**
De hoofdregel van de Algemene verordening gegevensbescherming eist dat persoonsgegevens op behoorlijke en zorgvuldige wijze en in overeenstemming met de wet worden verwerkt.
De AVG 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 ter beschikking stelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens. Een persoonsgegeven in de zin van de AVG 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 telefoon, 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 be-

richten – 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 internetsite 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 vertrouwelijke informatie
Controle op het uitlekken van vertrouwelijke informatie 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**
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. De beoordeling hiervan ligt bij de leidinggevende.

**Artikel 5**
Behoeft geen toelichting.

**Artikel 6**
Werknemers mogen het internetsysteem voor persoonlijke doeleinden gebruiken, mits dit niet storend is voor de dagelijkse werkzaamheden en het computernetwerk. De beoordeling hiervan ligt bij de leidinggevende.

**Artikel 7**
Behoeft geen toelichting.

**Artikel 8**
Werknemers mogen telefoons voor persoonlijke doeleinden gebruiken, mits dit niet storend is voor de dagelijkse werkzaamheden. De beoordeling hiervan ligt bij de leidinggevende.

**Artikel 9**
Behoeft geen toelichting.

**Artikel 10**
Wanneer de leidinggevende constateert dat een werknemer zich schuldig maakt aan verboden gebruik van het telefoon, e-mail en/of internetsysteem, bespreekt hij dit onmiddellijk met de betrokken werknemer. Daarbij wordt de werknemer gewaarschuwd voor de (rechtspositionele) consequenties, zoals vermeld in hoofdstuk 16 CAR/UWO die het verboden gebruik van het e-mail en/of internetsysteem voor hem kan hebben. De leidinggevende kan bijvoorbeeld wijzen op de risico's, zoals ontslag, die verbonden zijn aan verboden gebruik van het internet.

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.

**Artikel 11**
Met verkeersgegevens wordt bedoeld dat in eerste instantie er wordt gefilterd op woordgebruik en omvang in datagebruik. De berichten worden dus niet direct inhoudelijk gelezen.

**Artikel 12**
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.

**Artikel 13**
Tegen het opleggen van disciplinaire maatregelen/straffen kan op basis van de Algemene Wet Bestuursrecht (Awb) bezwaar en beroep worden aangetekend.

**Artikel 14**
Bij onvoorziene omstandigheden beslist het Dagelijks Bestuur.

**Artikel 15**
Behoeft geen toelichting.