

Bijlage 2

Toelichting bij Regeling Gebruik Elektronische Communicatiemiddelen Gemeente Maastricht

Inleiding

De Werknemers van de gemeente Maastricht maken bij het uitvoeren van hun werkzaamheden gebruik van Elektronische communicatiemiddelen, zoals e-mail en internet. De gemeentelijke werkplekken zijn voorzien van een pc waarop Werknemers kunnen inloggen op het gemeentelijke netwerk. Daarnaast heeft een groot deel van de Werknemers één of meer mobiele apparaten ontvangen (smartphone, tablet etc.) en kan er vanuit huis worden ingelogd op de gemeentelijke werkomgeving zodat zij hun taken plaats en tijd onafhankelijk kunnen uitvoeren.

Om het gebruik van deze middelen in goede banen te leiden en hierover duidelijk beleid te voeren, is de *Regeling Gebruik Elektronische Communicatiemiddelen Gemeente Maastricht* en deze bijbehorende toelichting vastgesteld. In deze regeling worden de rechten en verplichtingen van Werknemers bij het gebruik van de ter beschikking gestelde Elektronische communicatiemiddelen vastgelegd en beschreven hoe de monitoring en controle op dit gebruik plaatsvindt. Gestreefd wordt naar een goede balans tussen controle op verantwoord gebruik van deze middelen en bescherming van de privacy van Werknemers bij de uitvoering van hun werkzaamheden.

Uiteraard dient zowel het gebruik van als de controle op het gebruik van de Elektronische communicatiemiddelen te voldoen aan de van toepassing zijnde wet- en regelgeving waaronder de Algemene Verordening Gegevensbescherming (AVG).

Dit betekent onder meer dat het verwerken van persoonsgegevens in het kader van de controle op het gebruik van de Elektronische communicatiemiddelen alleen mogelijk is als hiervoor een wettelijke grondslag is zoals opgenomen in artikel 6 van de AVG. Verder dient een verwerking van persoonsgegevens op grond van deze regeling altijd te voldoen aan de wettelijke eisen van proportionaliteit en subsidiariteit en dienen de rechten die de AVG aan de betrokkenen (werknemers) geeft te zijn gewaarborgd.

Vanzelfsprekend zal de werkgever, indien dit gelet op de AVG en de richtsnoeren van de Autoriteit Persoonsgegevens verplicht is, een Gegevensbeschermingseffectbeoordeling (GEB)¹ uitvoeren voordat met een verwerking van persoonsgegevens wordt begonnen.

Artikelsgewijze toelichting

Artikel 1 onder b. Werkgever

De Werkgever is de gemeente Maastricht. De uitvoering van deze regeling is gemandateerd aan de gemeentesecretaris/algemeen directeur als hoogste Werknemer van de Werkgever.

¹ Instrument om voordat met het verwerken van persoonsgegevens wordt begonnen de privacy risico's in kaart te brengen en, indien nodig, extra maatregelen te treffen om deze risico's te beperken.

Artikel 1 onder c. Werknemer

Het begrip Werknemer dient ruim te worden uitgelegd en omvat alle natuurlijke personen die arbeid verrichten voor de gemeente Maastricht (de Werkgever) en aan wie Elektronische communicatiemiddelen ter beschikking zijn gesteld door de Werkgever. Hieronder vallen in ieder geval:

- personen in dienst van de gemeente Maastricht (ook met nul-urencontracten);
- personen die op basis van een uitzend- of detacheringsovereenkomst of overeenkomst van opdracht werkzaam zijn bij de gemeente Maastricht;
- personen die de gemeente Maastricht heeft uitgeleend of gedetacheerd bij andere organisaties;
- personen die anders dan op basis van een arbeidsovereenkomst werkzaam zijn voor of binnen de gemeente Maastricht, zoals zelfstandigen zonder personeel (ZZP'ers), stagiaires en vrijwilligers.

Artikel 1 onder d. Elektronische communicatiemiddelen

Hierbij kan bijvoorbeeld gedacht worden aan (zonder limitatief te willen zijn) een smartphone, tablet, laptop en softwarebestanden zoals e-mail, internet, intranet en de mogelijkheid om via een virtual private network (vpn verbinding) in te loggen op de gemeentelijke werkplek vanuit huis of een andere locatie buiten de gemeentelijke gebouwen.

Artikel 1 onder h. Onrechtmatig gebruik dan wel misbruik van elektronische communicatiemiddelen

Van Onrechtmatig gebruik dan wel misbruik is sprake indien in strijd wordt gehandeld met deze regeling of andere wet- en regelgeving of in geval een inbreuk wordt gemaakt op een recht. Bij een inbreuk op een recht gaat het om een inbreuk op een persoonlijkheidsrecht of vermogensrecht. Voorbeelden van persoonlijkheidsrechten zijn het recht op privacy en het recht op lichamelijke integriteit. Een voorbeeld van een vermogensrecht is het eigendomsrecht.

Artikel 3. Doeleinden

Het verwerken van Persoonsgegevens betreffende het gebruik van de Elektronische communicatiemiddelen is alleen mogelijk voor de in dit artikel omschreven doeleinden. Hierbij geldt als uitgangspunt dat de aard, omvang en vorm van de persoonsgegevens die zullen worden verwerkt in redelijke verhouding dienen te staan met het doel van de verwerking (proportionaliteit) en dat het verwerken van de persoonsgegevens niet meer inbreuk mag maken op de belangen van de Werknemer(s) dan strikt noodzakelijk is (subsidiariteit).

Artikel 5. Uitgangspunten gebruik Elektronische communicatiemiddelen

Lid 1 en 2. Zakelijk- en privégebruik

Werknemers gebruiken de ter beschikking gestelde Elektronische communicatiemiddelen primair voor de aan hen opgedragen taak. Privégebruik van de aan Werknemers ter beschikking gestelde Elektronische communicatiemiddelen is toegestaan mits:

- het gebruik in overeenstemming is met deze regeling en de bruikleenovereenkomst;
- het uitvoeren van de aan de Werknemer opgedragen werkzaamheden en de goede werking van het netwerk en andere ICT-faciliteiten er niet onder leiden;
- het privégebruik het zakelijk gebruik niet overstijgt en;
- het privégebruik niet leidt tot extra kosten voor de Werkgever.

Het is niet toegestaan om deze Elektronische communicatiemiddelen uit te lenen/ter beschikking te stellen aan derden, waaronder gezinsleden, die niet werkzaam zijn voor onze gemeente. Daarnaast mogen op de ter beschikking gestelde apparaten allen applicaties worden gedownload die niet verplichten tot het accepteren van bepaalde voorwaarden waardoor data, waaronder persoonsgegevens, gedeeld moeten worden met de leverancier van de applicatie.

Lid 3. Goed werknemerschap

Van Werknemers wordt verwacht dat zij zorgvuldig omgaan met de ter beschikking gestelde Elektronische communicatiemiddelen. De Werknemers dienen de instructies van de Werkgever over het omgaan met de Elektronische communicatiemiddelen op te volgen en bij het gebruik van de middelen interne voorschriften zoals deze regeling en landelijke wetgeving zoals de Algemene Verordening Gegevensbescherming (AVG) naleven.

Als Werkgever eisen wij bijvoorbeeld dat de Werknemers de Elektronische communicatiemiddelen altijd zorgvuldig opbergen en niet delen met anderen. Ook verwachten wij dat de Werknemers ervoor zorgen dat vertrouwelijke informatie niet langer op de middelen wordt opgeslagen dan strikt noodzakelijk is en dat de e-mailbox regelmatig wordt opgeschoond.

Kortom, de Werknemers dienen netjes om te gaan met de ter beschikking gestelde Elektronische communicatiemiddelen en zullen daarbij alles doen wat nodig is om schade te voorkomen en te beperken (goed werknemerschap).

Lid 4. Vertrouwelijkheid en beschikbaarheid

(Persoons)gegevens die worden verwerkt op de ter beschikking gestelde Elektronische communicatiemiddelen moeten goed beveiligd en vertrouwelijk blijven. De gegevens dienen te worden beschermd tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging.

Artikel 6. Het gebruik van Elektronische communicatie- en informatiemiddelen

Lid 1. Versleuteld versturen

Indien wij Persoonsgegevens versleuteld² versturen naar afzenders buiten de gemeente Maastricht, dient hiervoor gebruik te worden gemaakt van het door de gemeente ter beschikking gestelde programma. Dit is momenteel het programma Cryptshare. Krijgen wij van afzenders Persoonsgegevens gestuurd die versleuteld zijn met een ander versleutelprogramma, dan mag dit programma worden gebruikt voor het versleuteld versturen/beantwoorden van berichten aan die afzender.

Lid 3. Archivering en vernietiging

Op de archivering en vernietiging van Persoonsgegevens zijn de Archiefwet. De AVG, de Selectielijst gemeenten en intergemeentelijke organen 2020 of een geactualiseerde versie van deze selectielijst van toepassing.

Lid 10. Gebruik middelen

Deze opsomming is bedoeld om aan te geven welk gebruik van de ter beschikking gestelde Elektronische communicatiemiddelen in ieder geval niet is toegestaan. Dit is geen limitatieve opsomming.

Lid 10 sub a & d

Een Werknemer dient, voor zover dit redelijkerwijs van hem kan worden verwacht, ervoor te zorgen dat hij geen pornografisch materiaal en/of bericht ontvangt die (kunnen) aanzetten tot haat en/of geweld. Hiermee wordt ook bedoeld dat een Werknemer aan de afzenders van deze berichten laat weten dat hij deze niet wenst te ontvangen en/of hulp vraagt bij de betreffende gemeentelijke afdeling³ om de ontvangst van deze berichten te stoppen.

Lid 11. Uitzondering

Hierbij dient gedacht te worden aan Werknemers die taken uitvoeren op het gebied van ICT en bevoegd zijn in opdracht van de Werkgever onderzoek te doen naar het gebruik van de ter beschikking gestelde Elektronische communicatiemiddelen. Het kan dan bijvoorbeeld gaan om onderzoek naar het downloaden van illegale software of het versturen van discriminerende berichten.

Artikel 7. Continuïteit van de werkzaamheden

Het is in geval van uitdiensttreding of langdurige afwezigheid van een (ex-)Werknemer van belang dat de continuïteit van de bedrijfsvoering en dienstverlening geborgd is. Het kan

² De inhoud van het bericht is niet zichtbaar en de ontvanger van het bericht is de enige die dit kan openen door gebruik te maken van de aan hem/haar verstrekte "sleutel," zijnde een code die wordt verstuurd via een sms bericht.

³ Bij de inwerkingtreding van deze regeling is dit de Servicedesk (6050).

daarom noodzakelijk zijn om toegang tot de mailbox of bestanden te krijgen. Uiteraard wordt hierbij in alle gevallen rekening gehouden met de belangen van de (ex-)Werknemer. Er zal altijd naar worden gestreefd om de werknemer om toestemming te vragen en te informeren over het feit dat toegang tot de mailbox en/of bestanden noodzakelijk is in het kader van het bedrijfsbelang. Bovendien zullen E-mailberichten die de titel "persoonlijk" dragen dan wel zijn opgeslagen in een map "persoonlijk" of een soortgelijke benaming niet worden gelezen. Werknemers zullen, onder meer in de communicatie over deze regeling, worden geadviseerd om privéberichten zo snel mogelijk te verwijderen en indien dit niet wenselijk is, op te slaan in een aparte map in de mailbox of de hiervoor te gebruiken directory in de gemeentelijke werkomgeving met de benaming persoonlijk of privé. Een map die een dergelijke naam draagt kan voor de doelen zoals bedoeld in dit artikel 7 niet worden geopend. Indien een werknemer mocht komen te overlijden, zullen zijn directe nabestaanden in de gelegenheid worden gesteld om bovengenoemde mappen in te zien en op te schonen.

Artikel 8. Extern gebruik Elektronische communicatiemiddelen

Lid 3. Openbare wifi-netwerken

Onder openbare wifi-netwerken wordt verstaan wifi-netwerken die voor het publiek toegankelijk zijn. Het gaat dus om een wifi-netwerk waarmee iedereen verbinding kan maken. Gedacht kan bijvoorbeeld worden aan wifi-netwerken van een café, hotel, luchthavens, trein of bus. Deze wifi-netwerken mogen alleen worden benaderd via de gemeentelijke VPN verbinding. Op het moment dat deze regeling wordt vastgesteld is dit de VPN-verbinding die tot stand wordt gebracht door in te loggen via Cisco AnyConnect Secure Mobility Client en VMware Horizon.

Artikel 10. Controle algemeen

Controle op het gebruik van de ter beschikking gestelde Elektronische communicatiemiddelen is niet verboden, maar er dient aan een aantal voorwaarden te worden voldaan. De Werkgever is verplicht om voorafgaande aan de mogelijke controle duidelijk vast te leggen waarvoor het noodzakelijk is om een controle uit te voeren en dus persoonsgegevens te verwerken (noodzakelijkheidsvereiste). De Algemene Verordening Gegevensbescherming(AVG) spreekt over welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Daarnaast dient de controle te voldoen aan proportionaliteit en subsidiariteit. Hiermee wordt bedoeld dat de aard, omvang en vorm van de controle in redelijke verhouding dient te staan tot het doel van de controle (proportionaliteit) en dat de controle niet meer inbreuk mag maken op de (privacy)belangen van Werknemers dan strikt noodzakelijk is (subsidiariteit). Er dient dus altijd een belangenafweging plaats te vinden tussen het belang van een controle enerzijds en het belang van de betrokken Werknemer anderzijds. Deze belangenafweging dient te worden vastgelegd.

Controles worden zo beperkt mogelijk gehouden. Voor het verkrijgen van inzicht in de mate van gebruik van de ter beschikking gestelde Elektronische communicatiemiddelen blijft de controle beperkt tot Verkeersgegevens die informatie bevatten over het totale gebruik van de Elektronische communicatiemiddelen. Deze gegevens zijn niet herleidbaar tot individuele personen. Kennisname van de inhoud van de gegevens op persoonsniveau is in dat geval namelijk niet noodzakelijk.

Indien dit op grond van de hiervoor geldende regels noodzakelijk is zal er voorafgaande aan de uit te voeren controle een gegevensbeschermingseffectbeoordeling worden uitgevoerd.

Artikel 11. Wijze van controle op individueel niveau

Lid 1. Gerichte controle op individueel niveau

Bij een concreet vermoeden dat een Werknemer Onrechtmatig gebruik dan wel misbruik maakt van de ter beschikking gestelde Elektronische communicatie kan een gerichte (inhoudelijke) controle op individueel niveau plaatsvinden. In dit artikel wordt geregeld wanneer een dergelijke controle mogelijk is.

Indien het gelet op de aard van het concrete vermoeden mogelijk en zinvol is, zal er altijd als eerste worden gekozen voor een controle van de Verkeersgegevens op individueel niveau. Er wordt bij deze controle nog niet op inhoud gecontroleerd. Gekeken wordt of er op grond van de Verkeersgegevens meer duidelijkheid kan worden verkregen over mogelijk misbruik dan wel onrechtmatig gebruik van de ter beschikking gestelde Elektronische communicatiemiddelen. De Verkeersgegevens kunnen bijvoorbeeld duidelijk maken of bepaalde niet aan het werk te relateren websites onevenredig vaak wordt geraadpleegd.

Lid 2, lid 3 en lid 4. Informeren en toestemming gerichte inhoudelijke controle

Bij het uitvoeren van een gerichte inhoudelijke controle is het uitgangspunt dat de Werknemer hierover wordt geïnformeerd.

Er kan van het informeren van de Werknemer worden afgezien als er sprake is van een redelijke verdenking van een Strafbaar feit en tevens aan alle andere eisen wordt voldaan die de Autoriteit Persoonsgegevens aan een dergelijke controle stelt. Deze voorwaarden zijn opgenomen in lid 2 en luiden als volgt:

- a. Er is een redelijke verdenking dat de Werknemer een strafbaar feit pleegt en daarmee een zwaarwegend belang voor de Werkgever bij het onderzoek;
- b. Het ondanks diverse inspanningen niet mogelijk is gebleken om een einde te maken aan het vermoedelijke Strafbare feit.
- c. Het is niet mogelijk om het onderzoek uit te voeren op een wijze die minder inbreuk maakt op de privacybelangen van de betrokken Werknemer;

- d. Er redenen zijn om aan te nemen dat het vooraf informeren van de Werknemer over het uit te voeren onderzoek, dit het onderzoek zal belemmeren dan wel onmogelijk maken.

Van het bij sub d genoemde is bijvoorbeeld sprake als het informeren van de medewerker ertoe kan leiden dat bewijs wordt weggemaakt.

Aangezien het uitvoeren van een gerichte inhoudelijke controle naar het gebruik van de Elektronische communicatiemiddelen een zwaar middel is, dient de gemeentesecretaris/algemeen directeur toestemming te geven voor een dergelijke controle. Bovendien wordt in de toestemming bepaald gedurende welke tijdvak deze inhoudelijke controle mag plaatsvinden. Er zal altijd naar worden gestreefd om deze periode zo kort mogelijk te houden.

Verder vereist dit zware middel een zorgvuldige belangenafweging tussen het organisatiebelang en de belangen van de betreffende Werknemer. Om deze reden is in de regeling bepaald dat in de toestemming wordt vastgelegd waarom bij de uit te voeren inhoudelijke controle de inbreuk op de (privacy)belangen van de betreffende Werknemer(s) gerechtvaardigd is.

Indien een werknemer niet vooraf wordt geïnformeerd over de uit te voeren controle zal in de toestemming tevens worden gemotiveerd dat aan alle voorwaarden die zijn opgenomen in lid 2 wordt voldaan.

Voor de duidelijkheid wordt in dit kader opgemerkt dat het continue heimelijk controleren/monitoren van Werknemers op grond van de AVG en de richtlijnen van de Autoriteit Persoonsgegevens niet is toegestaan.

Lid 6. Gerichte inhoudelijke controle in beginsel uitgesloten

Een aantal werkzaamheden zijn in beginsel uitgesloten van een gerichte inhoudelijke controle. Het betreft als eerste een gerichte inhoudelijke controle van de elektronische communicatiemiddelen die aan een werknemer ter beschikking zijn gesteld voor de uitvoering van zijn werkzaamheden als OR-lid of als medewerker van het ambtelijk secretariaat van de ondernemingsraad. Deze bepaling sluit aan bij het gestelde in artikel 17 van de Wet op de Ondernemingsraden en volgt het standpunt van de Autoriteit Persoonsgegevens in deze.

In het Landelijk Overleg Gemeentelijke Arbeidsvoorwaarden is geconcludeerd dat de leden van het Georganiseerd Overleg zich in een soortgelijke positie bevinden als de OR-leden. Het Georganiseerd Overleg is inmiddels opgeheven en heeft plaatsgemaakt voor de Commissie voor het Lokaal Overleg. Echter, de bovengenoemde conclusie over de positie van de voormalige GO-leden geldt ook voor de Werknemers die deel uitmaken van de Commissie voor het Lokaal Overleg. Om die reden is besloten dat lid 5 ook van toepassing is op deze Werknemers.

Daarnaast vinden we het als Werkgever belangrijk dat Werknemers zich veilig voelen als zij informatie delen met een medewerker die één van de overige in deze bepaling genoemde werkzaamheden vervult. Dit betreft onder meer de contacten van Werknemers met de vertrouwenspersonen. De voor deze werkzaamheden ter beschikking gestelde Elektronische communicatiemiddelen, zoals bijvoorbeeld de mailbox van het Meldpunt Integriteit & Klachten (dus niet de persoonlijke mailbox van de leden van dit meldpunt) zijn daarom ook in principe ook uitgesloten van een gerichte inhoudelijke controle.

Lid 7 besluit over uit te voeren inhoudelijk onderzoek

Indien hiervoor zwaarwegende redenen aanwezig zijn, een redelijke verdenking van een Strafbaar feit, kan bij hoge uitzondering worden besloten om ook de in het vorige genoemde Elektronische communicatiemiddelen te onderzoeken. De gemeentesecretaris/algemeen directeur en de portefeuillehouder integriteit dienen hier samen over te beslissen.

Artikel 12. Bewaring en verwijdering

Persoonsgegevens mogen niet langer bewaard worden dan noodzakelijk is voor het doel van de verwerking (opslagbeperking). Het is in het algemeen ook niet nodig om de persoonsgegevens lang te bewaren. Er wordt daarom naar gestreefd om de persoonsgegevens in ieder geval niet langer dan twaalf maanden te bewaren, tenzij het noodzakelijk is om de gegevens in het kader van het onderzoek en/of opleggen van maatregelen of hieruit voortvloeiende procedures langer te bewaren. Zodra een nader onderzoek is afgerond en dit niet leidt tot maatregelen en eventuele procedures, dienen de persoonsgegevens te worden verwijderd of te worden geanonimiseerd zodat zij niet meer herleidbaar zijn naar individuele personen.

Het kan zo zijn dat er gegevens zijn die om technische redenen niet kunnen worden verwijderd. In dat geval wordt onder verwijdering verstaan dat de gegevens niet meer mogen worden verstrekt/verwerkt dan wel te raadplegen zijn.

Artikel 13. Rechten van de Werknemer

Een weigering om te voldoen aan dit verzoek is een besluit in de zin van artikel 1:3 van de Wet Algemene wet bestuursrecht en is vatbaar voor bezwaar en beroep.

Artikel 14 Sancties

Overtreding van deze regeling, hetgeen ook tot een overtreding leidt van de Gedragscode ambtelijke organisatie, kan voor Werknemers in dienst van de Werkgever in het uiterste geval een (dringende) reden zijn voor beëindiging van de arbeidsovereenkomst.

Wanneer de Werkgever constateert dat een Werknemer zich schuldig maakt aan overtreding van deze regeling, bespreekt hij dit onmiddellijk met de betrokken Werknemer. Daarbij wordt de werknemer direct gewaarschuwd voor de (arbeidsrechtelijke) consequenties die de

betreffende overtreding van de regeling voor hem kan hebben. De (arbeidsrechtelijke) gevolgen van een overtreding zijn afhankelijk van de aard en de ernst van de overtreding.

In geval van overtreding door personen die (betaalde of niet-betaalde) werkzaamheden voor de Werkgever verrichten, anders dan op grond van een arbeidsovereenkomst met de Werkgever, kunnen maatregelen worden genomen waardoor deze personen (tijdelijk) geen beschikking meer hebben over (een deel van) de Elektronische communicatiemiddelen of kan worden overgegaan tot beëindiging van hun werkzaamheden voor de Werkgever. Ook kunnen er maatregelen worden genomen om de schade die is ontstaan door overtreding van deze regeling te verhalen op de betreffende persoon. Dat laatste kan ook gelden voor Werknemers in dienst van de Werkgever.

Aangifte bij de politie behoort eveneens tot de mogelijkheden.