
MOBIELE APPARATUUR

Protocol

06.2.1 mobiele apparatuur

Bedrijfsvertrouwelijk

Gemeente Almere



Status	Vastgesteld is versie 1.0
Versie	2.0, wijziging naar BIO (i.p.v. BIG)
Ingangsdatum	21-12-2016
Reviewdatum	31-12-2022
Opdrachtgever	Gemeente Almere
Team/taakveld	CIO-Office / Informatieveiligheid
Auteur(s)	J.A. Blok, CISO S. Antonius, Senior Juridisch adviseur

Aanleiding

Binnen de gemeente Almere is het plaats- en tijdsafhankelijk werken inmiddels ingevoerd. Waar mogelijk en wenselijk werken we volgens dit uitgangspunt. Hierdoor worden de mobiele apparaten (hierna: mobile devices) gangbaarder en noodzakelijker. Ook zetten steeds meer medewerkers hun privé apparaten in ten behoeve van het werk. De gemeente Almere wil ruimte geven aan wat nodig of mogelijk is voor een medewerker, team, afdeling of dienst. Hierbij wordt vertrouwd op de (vak)kennis en professionaliteit van allen om bewust om te gaan met de mobile devices. Daarnaast blijft het belangrijk gegevens en informatiehuishouding worden beheerd.

De gemeente heeft zich gecommitteerd aan de Baseline Informatiebeveiliging Overheid (BIO). We voeren dit gefaseerd in. Op grond van de BIO moeten er regels worden vastgesteld, gedocumenteerd en geïmplementeerd voor aanvaardbaar gebruik van informatie en bedrijfsmiddelen die verband houden met ICT-voorzieningen. Er geldt op grond van de Algemene Verordening Gegevensbescherming een meldplicht voor datalekken. De Autoriteit Persoonsgegevens kan tevens hoge boetes opleggen bij het niet naleven van wettelijke bepalingen. Om de veiligheid van de gemeentelijke data te borgen en om aan de wettelijke verplichtingen te voldoen is normering van het gebruik van mobile devices aangewezen. De gemeente kent de “Algemene bepalingen gebruik mobile devices”, welke bepalingen van toepassing zijn op het gebruik van alle door of namens de gemeente verstrekte devices en/of informatie.

Er dient in aanvulling hierop binnen de gemeente ook een overkoepelend protocol te zijn voor het gebruik van alle mobile devices, ongeacht of dit privébezit van de medewerker is. Dit protocol voorziet daarin.

Op 17 juli 2017 heeft de Ondernemingsraad met dit protocol ingestemd.

Reikwijdte

Dit protocol ziet toe op het gebruik van alle mobile devices door (externe) werknemers en collegeleden van de gemeente.

Aan zzp-ers worden om fiscale redenen geen mobile devices door de gemeente verstrekt. Het protocol is derhalve niet van toepassing op zzp-ers, die werkzaamheden voor de gemeente verrichten.

Er wordt geen onderscheid gemaakt tussen mobile devices uitgegeven door of namens de gemeente en eigen mobile devices van werknemers/medewerkers (Bring Your Own Device). Mobile devices worden in beide toepassingsvormen steeds meer gebruikt binnen de gemeente, waardoor in toenemende mate data van de gemeente op de devices te vinden is. In alle gevallen blijft de data “eigendom” van de gemeente. Dit protocol is van toepassing op alle gebruikers van mobile devices die toegang hebben tot gemeentelijke informatie.

Belang

Het is van belang om veilig om te gaan met mobile devices en de gemeentedata die erop kan staan, omdat mobile devices:

- een besmetting met malware kunnen oplopen en daarmee de gehele gemeente kunnen infecteren (het mobile device wordt door hackers gebruikt);
- met gemeentedata fysiek zoekraken of worden gestolen. Dit kan leiden tot een datalek, dataschade en vervangschade van het apparaat;
- door malware hoge telefoonkosten kunnen veroorzaken;
- in sommige gevallen kunnen worden gebruikt om informatie van de gemeente te benaderen. Dit levert mogelijk privacy- en vertrouwelijkheidsrisico's op.

Management van mobile devices

Het management van mobile devices (mobile device management (MDM)) is het stelsel van maatregelen, procedures en ondersteunende producten dat het mogelijk maakt om mobile devices binnen gemeentes veilig te kunnen gebruiken. De maatregelen staan beschreven in de BIO.

MDM is van toepassing op de alle mobile devices, zowel in privé- als gemeentelijk eigendom.

Met MDM-software kan de gemeentelijke informatie van het mobile device (selectief) op afstand verwijderd worden. Hierdoor kan voorkomen worden dat onbevoegden of kwaadwillende bij de informatie komen. In het kader van informatieveiligheid worden alle door de gemeente verstrekte mobile devices voorzien van MDM-software. Zodra een medewerker zijn zakelijke mail (en / of zakelijke agenda) wil inzien op een mobile device dient de MDM-software van de gemeente Almere geïnstalleerd en geconfigureerd te zijn op het device.

Bring Your Own Device (BYOD)

BYOD houdt in dat medewerkers van de gemeente eigen apparaten, zoals bijvoorbeeld mobiele telefoons, iPads en laptops, kunnen gebruiken voor hun werk. Deze apparaten kunnen onderweg, maar ook op kantoor worden gebruikt. Vertrouwelijke informatie van de gemeente kan bekeken en opgeslagen worden op deze mobile devices. Doordat de gemeente “data-eigenaar” blijft, is het noodzakelijk dat er nadrukkelijk **toestemming** door de leidinggevende voor zakelijk gebruik wordt gegeven. Hieraan zijn geen rechten te ontleen, ondersteuning wordt op best-effort gegeven. De medewerker is verantwoordelijk voor registratie van het device bij het Servicedesk ICT.

Aan het zakelijk gebruik van BYOD worden minimaal de volgende eisen gesteld:

- laatste updates van het Operating Systeem;
- Wachtwoordauthenticatie door gebruikmaking van een sterk wachtwoord;
- *jailbreak¹, rooten van Android devices en ontwikkelaars unlock* is niet toegestaan;
- mogelijkheid om het apparaat op afstand selectief² te wissen en/of de toegang tot gemeentelijke data te blokkeren (MDM);
- medewerkers die zelf een apparaat meenemen naar het werk, zijn zelf (financieel) verantwoordelijk voor verzekering tegen diefstal, het onderhoud en beheer.

De gebruiker van BYOD is verplicht om deze eisen toe te passen.

De gemeente kan het gebruik controleren in geval van:

- klachten over het gebruik;
- een redelijk vermoeden van wangedrag of onrechtmatig gebruik. Er wordt voor een aantal functies een uitzondering gemaakt. Een uitwerking hiervan staat in het operationele beleid mobiele apparatuur.

Controle dient ter voorkoming van onrechtmatig gebruik, hierbij zal gegevensminimalisatie uitgangspunt zijn.

1

Jailbreak is het mogelijk maken van het draaien van niet goedgekeurde apps op een iOS apparaat, waardoor ook malware gedraaid kan worden; Rooten is het proces dat het mogelijk maakt dat men meer rechten krijgt op het apparaat (Android) en daardoor het complete besturingssysteem kan wijzigen of vervangen, en daarmee malware introduceren en gemeentelijke beveiligingsinstellingen te omzeilen.

² Zo kunnen de gemeentelijke gegevens (e-mail plus aangehaakte documenten, agenda en contacten) worden gewist en (indien gewenst) de persoonlijke gegevens worden behouden.

Verlies en/of diefstal

Diefstal c.q. verlies van een apparaat met gemeentelijke data dient zo snel mogelijk maar uiterlijk binnen 24 uur te worden gemeld bij het Servicedesk ICT, waarna het apparaat (selectief) kan worden gewist en/of de toegang tot gemeentelijke data wordt geblokkeerd. Buiten kantoor tijden dient het verlies of diefstal middels de piketdienst gemeld te worden. Daarnaast moet er bij diefstal aangifte gedaan worden bij de politie.

Onrechtmatig gebruik

Het is verboden een door de gemeente verstrekt apparaat onrechtmatig te gebruiken. Onder onrechtmatig gebruik wordt verstaan:

- het bezoeken van internetfaciliteiten met pornografische, seksistische, discriminerende of aanstootgevende inhoud;
- het versturen van berichten aan een groot aantal medewerkers, kettingbrieven of kwaadaardige software, zoals virussen en spyware³;
- het downloaden of verzenden van illegale software.

Privégebruik mobile devices onder werktijd

Privégebruik van alle mobile devices is incidenteel toegestaan, mits dit gebruik in overeenstemming is met dit protocol en in geen geval storend is voor, dan wel ten koste gaat van, de dagelijkse werkzaamheden.

Controle gemeentelijke mobile devices

In het kader van optimalisering van de bedrijfsvoering en het voorkomen van strijdig gebruik en wangedrag, kunnen er op grond van een gerechtvaardigd belang periodiek controles worden uitgevoerd op het gebruik van door of namens de gemeente verstrekte mobile devices. Controle vindt in de eerste instantie plaats op het niveau van getotaliseerde gegevens. De gemeente heeft het recht om, indien de gemeente dit nodig acht, ook op detailniveau te controleren. Bij de controles zijn gegevensminimalisatie uitgangspunt.

Persoonsgegevens die zijn vastgelegd in het kader van toezicht en controle worden zo kort mogelijk en niet langer dan noodzakelijk bewaard. Enkel indien er een redelijk vermoeden bestaat van onrechtmatig gebruik, kunnen deze gegevens langer worden bewaard. Zodra een onderzoek is afgerond en dit niet tot maatregelen tegen een betrokkene heeft geleid, worden de gegevens direct verwijderd.

Controle op de naleving van dit protocol wordt, zo beperkt mogelijk uitgevoerd, zodat deze in redelijke verhouding staat tot het doel waarvoor deze wordt aangewend. De privacy van de medewerker wordt hierbij zo veel mogelijk gewaarborgd.

Medewerkers kunnen in verband met de naleving van dit protocol ter verantwoording worden geroepen. Het handelen in strijd met dit protocol kan als plichtverzuim aangemerkt.

Berichten op mobile devices en de Wet openbaarheid van bestuur

Zakelijke berichten die middels een mobile device worden uitgewisseld, via mail, sms of apps zoals chatapplicaties, kunnen op grond van de Wet openbaarheid van bestuur opgevraagd worden.

³ Virussen en spyware dienen wel gemeld te worden via de servicedesk en MijnICT
Versie: 2.0

Op zakelijke mobile devices is een alternatief voor Whatsapp voorhanden, bestaande uit een chatfunctionaliteit, waarbij met deelnemers binnen een besloten team kan worden gecommuniceerd.

Deze chatfunctionaliteit zal op alle zakelijke toestellen worden geïnstalleerd. Uitgangspunt is dat deze chatfunctionaliteit als voorkeurskanaal wordt gebruikt om te communiceren over zakelijke en bestuurlijke aangelegenheden.

Let wel, indien desondanks toch gebruik wordt gemaakt van Whatsapp voor zakelijke of bestuurlijke aangelegenheden, dan moet deze informatie ingeval van een Wob-verzoek door de gebruiker/ambtenaar/collegelid worden verstrekt.

Algemene bepalingen gebruik mobile devices

Inleiding

De gemeente Almere verstrekt aan medewerkers (hierna: gebruikers) ten behoeve van de uitoefening van de functie, mobile devices met bijbehorend abonnement en accessoires (hierna: apparatuur). Voorbeelden van apparatuur zijn mobiele telefoons, smartphones, laptops en tablets. De apparatuur wordt in bruikleen gegeven aan gebruiker. Op het gebruik van alle apparatuur zijn de onderhavige algemene bepalingen en het protocol mobiele apparatuur van toepassing. Eenmalige accordering van de onderhavige bepalingen door gebruiker geldt voor alle huidige en in de toekomst door de gemeente Almere in bruikleen te geven apparatuur en zakelijke abonnementen. Op dit document zijn ook het privacyreglement email en internetgebruik van toepassing.

1. Aard en uitvoering

Het type apparatuur, met het zakelijke abonnement, wordt door gemeente vastgesteld. Het type apparatuur (en het abonnement) is gespecificeerd en geadmistreerd bij de dienstverlener en in MijnHRM.

2. Rechten en plichten gebruiker

- a. Gebruiker verklaart de apparatuur in goede staat te hebben ontvangen en deze niet aan derden ter beschikking te stellen, te verpanden of op enigerlei andere wijze te vervreemden.
- b. Gebruiker is verantwoordelijk voor het in goede en representatieve staat houden van de apparatuur.
- c. Gebruiker dient alle zorgvuldigheid in acht te nemen ter voorkoming van beschadiging, diefstal of verlies van de apparatuur.
- d. Ter bescherming van de data op de apparatuur dient de gebruiker afdoende beschermingsmaatregelen te treffen door de (BYOD) apparatuur te voorzien van periodieke wachtwoorden, conform het gemeentelijke wachtwoordbeleid. Indien de apparatuur op het moment van bruikleen door de gemeente of dienstverlener reeds is voorzien van beveiliging, is het de gebruiker niet toegestaan om deze beveiliging te verwijderen of op andere wijze onbruikbaar te maken.
- e. Het is gebruiker niet toegestaan zonder toestemming van de gemeente wijzigingen in de configuratie van de apparatuur aan te brengen en/of illegale software te downloaden.
- f. Het is gebruiker niet toegestaan de apparatuur te gebruiken voor activiteiten die:
 - a) in strijd zijn met de bedrijfsdoelstellingen;
 - b) de persoonsgegevens die de gemeente verwerkt in gevaar (kunnen) brengen of het aanzien van de gemeente schade (kunnen) berokkenen;
 - c) de grenzen van betamelijkheid en fatsoen overschrijden.
- g. Gebruiker is op de hoogte dat gemeente het gebruik van de apparatuur (en het abonnement) periodiek controleert. Controle vindt in eerste instantie plaats op het niveau van getotaliseerde verbruiksgegevens. De gemeente behoudt zich het recht voor om, indien de gemeente dit nodig acht, ook op detailniveau te controleren.
- h. Gebruiker mag de apparatuur (en het abonnement) op basis van "Fair Use Policy" ook voor privé doeleinden binnen Nederland gebruiken. Dit houdt in dat de apparatuur (en het abonnement) naar redelijke maatstaven privé mag worden gebruikt. Zie, indien van toepassing, ook de Fair Use Policy van de desbetreffende dienstverlener.
- i. Bij excessief hoge telefoonkosten, gerelateerd aan privégebruik van de apparatuur met het daarbij behorende zakelijke abonnement, kan de gemeente de in rekening gebrachte kosten op de gebruiker verhalen.
- j. Gebruiker geeft op eerste verzoek van de gemeente tussentijds de apparatuur terug, indien er sprake is van onrechtmatig gebruik van de apparatuur of indien op enigerlei wijze in strijd met deze algemene bepalingen is/wordt gehandeld.

3. Telefoongedrag

- a. Gebruiker dient de GSM-gebruikersvoorschriften op locaties ten aanzien van klanten of andere relaties te respecteren.
- b. Het gebruik van de mobiele telefoon is niet toegestaan in de auto zonder gebruikmaking van een carkit, dan wel een handsfree set. Niet handsfree bellen wordt onder alle omstandigheden aangemerkt als bewust roekeloos handelen. De gemeente aanvaardt geen aansprakelijkheid voor zaak- of letselschade als gevolg hiervan, tevens zijn boetes voor rekening van gebruiker.
- c. Het is gebruiker niet toegestaan om een BYOD voor zakelijke (gemeentelijke) berichtgeving via sms danwel Whatsapp te gebruiken.

4. Reparatie

- a. Bij het optreden van storingen op door gemeente verstrekte apparaten en/of abonnementen dient de gebruiker zo snel mogelijk contact op te nemen met het Serviceplein ICT. Serviceplein ICT verwijst gebruiker, zo nodig, door.
- b. Reparatie en onderhoud aan de apparatuur wordt door de gebruiker geregeld via MijnICT. De daaraan verbonden kosten zijn voor rekening van de gemeente, tenzij wordt geconstateerd dat sprake is van een onzorgvuldig gebruik en/of nalatigheid. De gemeente is, onder omstandigheden, bevoegd de in bruikleen gegeven apparatuur te vervangen.

5. Diefstal en beschadiging

In geval van diefstal van de apparatuur is gebruiker verplicht dit zo spoedig mogelijk, doch uiterlijk binnen 24 uur, bij het Serviceplein ICT te melden. Gebruiker dient, in geval van diefstal, het apparaat onmiddellijk te laten blokkeren door het Serviceplein ICT. Gebruiker kan aansprakelijk worden gesteld voor schade aan de apparatuur ontstaan door verwijtbare nalatigheid of onachtzaamheid.

6. Termijn van gebruik

Gebruiker dient de apparatuur bij beëindiging van het dienstverband, of bij functiewijziging waarbij de apparatuur functioneel niet noodzakelijk is, uiterlijk op de laatste werkdag op eerste verzoek in volledige staat bij de leidinggevende te retourneren. Bij verzuim hiertoe, verbindt gebruiker zich tot betaling van de 'producten en dienstencatalogus'-waarde van de apparatuur aan gemeente.

7. Plichtsverzuim

Het handelen in strijd met de onderhavige algemene bepalingen kan als plichtverzuim aangemerkt.