BZK-aanbevelingen plaatsonafhankelijk werken met de BRP

Gemeenten (i.c. College van B&W) zijn verantwoordelijk voor de beveiliging van de gemeentelijke BRP-voorzieningen en bescherming van de BRP-gegevens in deze voorzieningen. Hierbij dienen gemeenten met ingang van 25 mei 2018 conform de Europese Algemene Verordening Gegevensbescherming (AVG) te handelen. Vanuit de rol als stelselverantwoordelijke en de toezichthoudende rol bij de inrichting, werking en beveiliging van de gemeentelijke BRP-voorzieningen, doet het ministerie van BZK specifieke aanbevelingen voor telewerken met de BRP. Telewerken met de BRP is mogelijk mits de gemeente naast het voldoen aan de geldende regelgeving BRP, duidelijke technische en organisatorische voorwaarden stelt en heldere gedragsregels formuleert ter beveiliging van persoonsgegevens tegen verlies of onrechtmatige bewerking of verkrijging.

Het telewerkbeleid van de gemeente dient ingericht te worden volgens de aanbevelingen van de Informatie Beveiligingsdienst (IBD) zoals deze zijn opgenomen in de handreikingen Telewerkbeleid en Mobile Device Management (MDM). Deze producten maken onderdeel uit van de operationele variant van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) en zijn te vinden op de website informatiebeveiligingsdienst.nl. Daarnaast doet BZK specifiek voor telewerken met de BRP aanvullende aanbevelingen betreffende de inrichting van de technische voorzieningen en gedragsregels rondom telewerken. Gemeenten worden aangeraden deze aanbevelingen toe te passen. De aanbevelingen zijn specifieke aanvullingen op de Handleidingen van de IBD en dienen niet op zichzelf staand te worden gezien. Daar waar de IBD meerdere mogelijkheden biedt voor invulling wijst BZK op een bepaalde inrichting. De voorwaarden voor telewerken met de BRP maken onderdeel uit van het jaarlijks wettelijke zelfevaluatie instrument (incl. ENSIA) bij gemeenten. De Autoriteit Persoonsgegevens is de toezichthouder op de bescherming van de persoonsgegevens in de BRP.

Risicoafweging Telewerken met BRP
Gemeenten dienen zich er bewust van te zijn dat telewerken met de BRP risico's bergt betreffende privacy en veiligheid.

De Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) is de basis voor de informatiebeveiliging voor alle gemeenten van Nederland. Een aanvullende risicoanalyse is binnen de BIG niet nodig zolang de BIG op de producten Telewerken en Mobile Device Management wordt toegepast. Als deze twee handreikingen gevolgd worden, dan is het ook voor de BRP mogelijk (in aanvulling op de wettelijke vereisten zoals opgenomen in de wet BRP, besluit BRP en LO BRP) om telewerken of mobiel werken voor een gemeente op een veilige manier in te richten en daarmee tijd- en plaatsonafhankelijk werken voor medewerkers van burgerzaken mogelijk te maken.

[zie ook informatiebeveiligingsdienst.nl]

***Informatiebeveiligingsbeleid telewerken*:**
Het informatiebeveiligingsbeleid van de gemeente moet geformuleerd worden. Voor telewerken dient de Handleiding Telewerkbeleid van de Informatiebeveiligingsdienst voor gemeenten (IBD) als voorbeeld. Voor plaatsonafhankelijk werken met de BRP moeten er regels binnen de gemeente geformuleerd en gehanteerd worden. Het doel is om te voorkomen dat de dienstverlening van de gemeente hinder ondervindt van de risico's in geval van gedeeltelijk of geheel verlies, beschadiging van data en/of programmatuur en hardware. Er dient binnen de gemeente ook nagedacht te worden over welke diensten wel, en welke diensten niet vanuit de thuiswerkplek of andere apparaten geraadpleegd mogen worden. Als telewerken wordt toegestaan dient er expliciet aandacht te zijn voor controle van de regels door het management.

Inrichting technische voorzieningen

- Maatregelen moeten in lijn zijn met de BIG (Telewerken en MDM)

- Door de gemeente moet beleid worden opgesteld met gedragsregels en een geschikte implementatie van de techniek voor telewerken.
- Voor werken op afstand is een thuiswerkomgeving beschikbaar of er wordt gebruik gemaakt van een mobiel apparaat zoals een laptop, een tablet of een smartphone. Toegang tot vertrouwelijke informatie wordt in alle gevallen verleend op basis van multifactor authenticatie.
- Mobiele bedrijfsapplicaties worden zo aangeboden of gebruikt dat er geen gemeentelijke informatie wordt opgeslagen op het mobiele apparaat (‘zero footprint’).
- Gemeentelijke informatie en bedrijfsinformatie van derde partijen die via het gemeentelijk platform wordt ontsloten dient te worden versleuteld bij transport en opslag, conform classificatie eisen.
- Beveiligingsmaatregelen hebben betrekking op zowel door de gemeente verstrekte middelen als privé-apparatuur ('bring your own device' (BYOD)). Op privé-apparatuur waarmee verbinding wordt gemaakt met het gemeentelijke netwerk is de gemeente bevoegd om beveiligingsinstellingen af te dwingen. Dit betreft onder meer: controle op wachtwoord, encryptie, aanwezigheid van malware, et cetera. Het gebruik van privé-apparatuur waarop beveiligingsinstellingen zijn verwijderd ('jail break', 'rooted device') is niet toegestaan.
- Op verzoek van de gemeente dienen medewerkers de installatie van software om bovenstaande beleidsregel te handhaven toe te staan (denk bijvoorbeeld aan ‘mobile device management software’). De beveiligingsinstellingen, zoals bedoeld in bovenstaande regel, zijn uitsluitend bedoeld ter bescherming van gemeentelijke informatie en integriteit van het gemeentelijke netwerk.
- In geval van dringende redenen kunnen noodmaatregelen worden getroffen, zoals wissen van apparatuur op afstand. Deze noodmaatregelen kunnen, voor zover dit noodzakelijk is, betrekking hebben op privémiddelen en privébestanden.

Gedragsregels rondom plaatsonafhankelijk werken met de BRP

- Beleid moet worden vastgesteld met daarin uitgewerkt welke systemen niet en welke systemen wel vanuit de thuiswerkplek of andere apparaten mogen worden geraadpleegd. Dit beleid moet in overeenstemming zijn met de IBD aanwijzing Mobile Device Management.
- Er zijn afspraken opgenomen over de rechten en plichten van de medewerker, alsook de mogelijke gevolgen bij een geconstateerde overtreding.
- De telewerkvoorzieningen zijn zo ingericht dat op de werkplek (thuis of op een andere locatie) geen bedrijfsinformatie wordt opgeslagen (‘zero footprint’) en mogelijke malware vanaf de werkplek niet in het vertrouwde deel terecht kan komen.
- Printen in niet vertrouwde omgevingen is niet toegestaan.
- Het is de telewerker verboden om bedrijfsinformatie lokaal op het privé-apparaat op te slaan.
- De medewerker is gehouden aan regels:
    - Illegale software mag niet worden gebruikt voor de uitvoering van het werk.
    - Er bestaat geen plicht de eigen computer te beveiligen, maar de gemeentelijke informatie daarop wel. Gezien zero footprint uitgangspunt zoals hierboven omschreven is het niet toegestaan/mogelijk om gemeentelijke informatie op de eigen computer te zetten
    - Het verbod op ongewenst gebruik in de (fysieke) kantooromgeving geldt ook als dat via de eigen computer in een thuissituatie plaatsvindt.
    - Het beeldscherm dient zodanig opgesteld te zijn dat ‘shoulder surfing’ niet mogelijk is.
- De telewerklocatie moet (als het gebruik van privé-apparaat wordt toegestaan) voorzien zijn van een:
    - Up-to-date virusscanner
    - Personal firewall
    - Anti malware tool
    - Screensaver beveiligd met een wachtwoord (zorg dat, als je de pc verlaat, de screensaver wordt geactiveerd)

    - Up-to-date besturingssysteem en applicaties.
- De telewerker dient te zorgen voor de aan hem beschikbaar gestelde apparatuur (zoals apparaat en authenticatie token), en zelf geen applicaties te installeren zonder toestemming van de beheerorganisatie.
- Er wordt aangegeven op welke locaties de telewerker mag telewerken. Zo is het verboden om vanuit een internetcafé of via een onbeveiligde (openbare) draadloze verbinding te telewerken.