Advies plaatsonafhankelijk werken met Burgerzakenprocessen

Werkgroep: Telewerken en Burgerzaken

Menno Kroesen, lid van de NVVB-commissie Persoonsinformatievoorziening)

Jan Otten, lid van de NVVB-commissie Persoonsregistratie

Janet van der Ree, voorzitter van de NVVB-commissie Persoonsinformatievoorziening

Ronald Zijlstra, strategisch adviseur bureau NVVB

Afgestemd met:

Informatiebeveiligingsdienst Nederlandse Gemeenten (Anita van Nieuwenborg, KING)

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties(Carel Aalbers van Rijksdienst voor Identiteitsgegevens en Yolanda Adel)

Bureau Digicommissaris (Erik Jonker)

Vereniging van Nederlandse gemeenten (Koen Wortman)

Inhoud

Inleiding 3
Reikwijdte 5
Bewerken en raadplegen 5
Van gemeentelijke database naar centrale database 5
Plaatsonafhankelijk werken door Burgerzaken 6
Beleid en risico-analyse 6
Risico's en maatregelen 6
Gedragsregels 7
Bewerken van gegevens 8
Uitgangspunten en voorwaarden bij autorisatie 8
Uitgangspunten en voorwaarden t.a.v. techniek 9
Bijlage 1: 11
Telewerkbeleid gemeente van IBD (BIG) 11
Bijlage 2: 12
Voorbeeld van documenten die plaatsonafhankelijk bewerken en raadplegen van persoonsgegevens ondersteunen 12
Voorstel aan het MT 12
Aanvraag thuiswerken met de BRP 14
Aanvraag autorisatie raadplegen, muteren en corrigeren BRP 15

Inleiding

Thuiswerken, Telewerken, Flexwerken, Het Nieuwe Werken; allemaal benamingen die wel gebruikt worden voor het werken anders dan in het kantoorgebouw van de gemeente. In dit advies noemen we het plaatsonafhankelijk werken. De definitie luidt: “Onafhankelijk van tijd en plaats werken met behulp van informatie- en communicatietechnologie (ICT), buiten de vaste werkomgeving van de gemeente”.

Thuiswerken of ‘langs de weg’ en in de buitendienst vraagt organisatie van de wijze waarop gemeentemedewerkers gebruik kunnen maken van de kantoorautomatisering en de toepassingssystemen die ze daarbij nodig hebben. Onvermijdelijk daarbij is ook de toegang tot digitaal opgeslagen gegevens. In het burgerzakendomein valt daarbij de basisregistratie personen (BRP) direct op en doemt het risico van privacyaantasting al gauw op.

Het recht op privacy is voor iedereen van groot belang. Dit belang wordt zeker gevoeld wanneer de privacy wordt geschaad en er vervelende gevolgen zijn.
Burgers kunnen een onveilig gevoel krijgen als gegevens over hen in handen zijn gekomen van anderen die daarop geen aanspraak kunnen en mogen maken. Burgers moeten erop kunnen vertrouwen dat hun persoonlijke gegevens bij de overheid in veilige handen zijn.
Erger is wanneer burgers ontdekken dat hun gegevens zijn gewijzigd door anderen die daartoe geen recht hadden. Burgers moeten altijd in control zijn over hun eigen gegevens en moeten kunnen weten wat er van hen is geregistreerd. Zij moeten op de hoogte zijn of worden gebracht van wijzigingen die in hun gegevens worden aangebracht. Die wijzigingen moeten zijn doorgevoerd op grond van de wet, als gevolg van de registratie van feiten over de burgerlijke staat of op grond van een eigen verzoek of aangifte. Burgers hebben correctierecht en kunnen langs die weg de overheid verzoeken gegevens te verbeteren.

Dat klinkt allemaal mooi, maar als er onbevoegde toegang tot gegevens plaatsvindt of onbevoegde wijziging van die gegevens, kan dat de burger veel schade berokkenen. Dit moet dus voorkomen worden, alhoewel dit niet voor 100% gegarandeerd kan worden.

Beheerders van privacygevoelige gegevens hebben de taak ervoor te zorgen dat de gegevens inhoudelijk op orde zijn en blijven maar ook dat deze zich in een veilige omgeving bevinden en dat de toegang beperkt is tot diegenen die de gegevens nodig hebben voor hun taakuitvoering. Zij krijgen ook slecht die gegevens die nodig zijn voor die taakuitvoering. Doelbinding dus.
Verder zal geregeld moeten worden op welke wijze toegang kan worden verschaft.

Gemeentemedewerkers gebruiken bij de toegang tot gemeentelijke systemen uiteenlopende apparaten, zoals desktop, laptop, tablet en smartphone. In dit advies noemen we het apparaat waarmee de gemeentemedewerker toegang verkrijgt simpelweg het *apparaat*.

Veel gemeenten kennen al vormen van plaatsonafhankelijk werken. Toch is er geen eenduidig beleid en als dat er al is, strookt het momenteel niet met het door het Rijk gewenst beleid. Binnen de kaders van de wet hebben gemeenten elk hierin een eigen verantwoordelijkheid.
Advies is om bij de naleving van dit ledenadvies en de daarin vermelde richtlijnen aan te haken bij de vragenlijst die ENSIA in het kader van de zelfevaluatie ontwikkelt. ENSIA staat voor Eenduidig Normatiek Single Information Audit (ENSIA), is nog in ontwikkeling en heeft tot doel verantwoordings- en auditinspanningen bij overheden te verminderen. In deze ENSIA wordt dan ook meting/controle van de beveiliging bij plaatsonafhankelijk werken meegenomen.

Dit advies beperkt zich tot het Burgerzakendomein en is voornamelijk gericht op de Basisregistratie personen en is aanvullend op het product Telewerkbeleid van de IBD[1]. IBD is een gezamenlijk initiatief van de Vereniging van Nederlandse Gemeenten (VNG) en het Kwaliteitsinstituut Nederlandse Gemeenten (KING) en actief sinds 1 januari 2013. Aanleiding voor de oprichting van de IBD vormen enerzijds de leerpunten uit een aantal grote incidenten op informatiebeveiligingsvlak en anderzijds de visie Digitale Overheid 2017. De IBD is er voor alle gemeenten en richt zich op bewustwording en concrete ondersteuning om gemeenten te helpen hun informatiebeveiliging naar een hoger plan te tillen. Het product Telewerkbeleid is als bijlage 1 toegevoegd aan deze notitie.

Daarnaast wordt aanbevolen om naast dit product ook de beveiligingsrichtlijnen van NCSC omtrent mobiele apparaten en webapplicaties mee te nemen.

De gemeente is zelf verantwoordelijk voor het opstellen, uitvoeren en handhaven van de regels. Hierbij geldt:

- Er is wetgeving waar altijd aan voldaan moet worden, zoals (niet uitputtend): BRP, SUWI, BAG, PUN en WBP, maar ook de Archiefwet.
- Er is een gemeenschappelijk normenkader als basis: de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG), waartoe de producten Telewerkbeleid, Mobile Device Management, Cloud Computing en Aanwijzing Logging behoren.
- De gemeente stelt dit normenkader vast, waarbij er ruimte is in de naleving van dat kader voor afweging en prioritering op basis van het ‘pas toe of leg uit’ principe.

Alle aanbevelingen en maatregelen, die reeds genoemd zijn in het product Telewerkbeleid van de IBD zijn van toepassing en worden in dit advies niet herhaald. Deze zijn al een prima uitgangspunt voor het opstellen van beleid voor telewerken.

Dit advies van de NVVB heeft het volgende doel:

Het onder verwijzing naar het product Telewerkbeleid ondersteunen van gemeenten bij het opstellen van een aanvullend beleid ten aanzien van het plaatsonafhankelijk werken met Burgerzakenprocessen waarbij de BRP wordt geraadpleegd en wordt bewerkt.

Werken op afstand is alleen aanvaardbaar als de privacy is gewaarborgd van personen van wie gegevens binnen dat werk worden verwerkt. De gemeente is bij de verwerking van persoonsgegevens in het algemeen gehouden aan de Wet Bescherming Persoonsgegevens. Als het om de BRP gaat is het de wet- en regelgeving van de BRP zelf die bepalend is. De verwerking van BRP-gegevens valt niet onder het regime van de WBP. Het toezicht op de uitvoering van de Wet BRP wel.

De gemeente kan plaatsonafhankelijk werken toestaan onder bepaalde voorwaarden die technisch en organisatorisch van aard zijn en ook met het duidelijk formuleren van gedragsregels hiertoe. Dit, om persoonsgegevens te beveiligen tegen verlies of onrechtmatige bewerking of verkrijging. De regels moeten volkomen helder zijn bij de gemeentemedewerkers en de gevolgen bij niet naleving van bijvoorbeeld gedragsregels moeten ondubbelzinnig bekend zijn.

In Bijlage 2 zijn voorbeelden van bestaande documenten opgenomen die een gemeente in Nederland heeft gebruikt om het telewerken voor Burgerzaken in te richten.

[1] Informatiebeveiligingsdienst Nederlandse Gemeenten

Reikwijdte

Bewerken en raadplegen

De reikwijdte van dit advies behelst het raadplegen en bewerken van persoonsgegevens die betrekking hebben op Burgerzakenprocessen.

Telewerkers hebben of alleen gegevens nodig voor de uitvoering van hun taken of zij hebben juist de taak om persoonsgegevens op te nemen, te wijzigen, aan te vullen of te corrigeren. Alleen gebruiken valt onder de noemer *Raadplegen*. Gegevens opnemen, wijzigen, aanvullen of corrigeren valt onder de noemer *Bewerken*.

Daarbij lijkt raadplegen minder ingrijpend dan bewerken. Het risico bij raadplegen is dat de gegevens in handen kunnen komen van iemand die daar geen recht op heeft. Het risico bij bewerken lijkt groter. Immers, als een niet geautoriseerd persoon gegevens van een geregistreerde kan wijzigen, kan dat dramatische privacy- of andere gevolgen hebben voor de geregistreerde.

Maar hoe dan ook zullen de maatregelen om risico's bij het raadpleegproces of bewerkingsproces in te dammen, vrijwel gelijk zijn.

Van gemeentelijke database naar centrale database

Tot medio 2018 zullen alle gemeenten nog gebruik maken van oude (GBA-)voorzieningen als het gaat om de BRP. De oude voorzieningen zijn de burgerzakensystemen die voldoen aan het Logisch Ontwerp GBA, thans versie 3.9. Dat betekent dat elke gemeente haar eigen database heeft met persoonsgegevens.

Als in 2018 de eerste gemeenten gaan aansluiten op de nieuwe BRP-voorzieningen betekent dat een feitelijke overdracht van het technisch beheer van de nu in de burgerzakensystemen opgeslagen persoonsgegevens naar het centrale systeem van BZK. Rechtstreekse toegang tot persoonsgegevens, al dan niet plaatsonafhankelijk, zal verschuiven van het lokale BRP-bestand naar het centrale deel, dan wel naar het lokale gegevensmagazijn van de gemeente. Dat betekent dat niet alleen de toegang tot persoonsgegevens binnen de wet- en regelgeving BRP geregeld moet worden maar dat ook toegang geregeld moet worden binnen de Wet Bescherming persoonsgegevens (Wbp) als het gaat om het gemeentelijke gegevensmagazijn.

Conclusie is dat bij het inrichten van veilig plaatsonafhankelijk werken in het Burgerzakendomein niet alleen gekeken moet worden naar de BRP, maar ook naar het gemeentelijk gegevensmagazijn.

Opgemerkt dient te worden dat in het gemeentelijk gegevensmagazijn niet alleen gegevens van personen zijn opgeslagen die in de gemeente wonen, maar ook die buiten de gemeente wonen, maar waarmee de gemeente een relatie onderhoudt. Verder bevat het gegevensmagazijn veelal meer gegevens over personen dan die in de BRP. De niet-BRP-gegevens worden ook wel aangehaakte gegevens genoemd.

De Meldplicht datalekken geldt niet voor de gegevensverwerking in de BRP, maar bij het plaatsonafhankelijk werken wordt ook gebruikgemaakt van persoonsgegevens die onder de werking van de Wbp vallen. Gegevens kunnen uit de BRP verstrekt zijn voor het uitvoeren van taken. Als vervolgens bij die uitvoering gegevens verloren gaan of 'weglekken' dan geldt de meldplicht wel.

Plaatsonafhankelijk werken door Burgerzaken

Voor plaatsonafhankelijk werken zijn beleid, operationele plannen en procedures nodig en een effectieve implementatie.

Het product Telewerkbeleid voorziet in gedragsregels en een inkadering van de techniek. Aanbevolen wordt dit over te nemen in de eigen gemeentelijke beleidsplannen.
De plannen bevatten een overzicht van welke maatregelen worden uitgevoerd, door wie en wanneer.
De procedures geven stapsgewijs aan op welke wijze een gemeentemedewerker toegang kan krijgen voor het plaatsonafhankelijk raadplegen en wat hij zelf doet of nalaat nadat hij toegang heeft gekregen.

Beleid en risico-analyse

Voordat een gemeente het beleidsplan op kan stellen zal zij een risicoanalyse moeten uitvoeren om de dreigingen en risico's voor de processen te analyseren. Het is aan te bevelen om daarvoor professionele begeleiding in te huren. Wellicht zijn er in iedere gemeente dreigingen en risico's te ontdekken die aanvullend zijn op wat er het product Telewerkbeleid is opgenomen. Vervolgens kunnen daarvoor aanvullende maatregelen worden bepaald.

Risico's en maatregelen

De belangrijkste risico's met betrekking tot plaatsonafhankelijk werken en welke maatregelen kunnen worden genomen om het risico te verlagen, staan in het product Telewerkbeleid van IBD.

De schakels van de telewerkketen die daarin genoemd zijn tussen medewerker en de ICT-infrastructuur van de gemeente en de daarbij in het oog springende risico's en maatregelen, zijn:

- De telewerklocatie
- De telewerkvoorziening zoals een desktop, laptop, tablet of smartphone. In het vervolg aangeduid met 'apparaat'.
- De verbinding tussen het apparaat en de ICT-infrastructuur van de gemeente
- De systemen die door de telewerker benaderd kunnen worden
- De informatie die aan de telewerker beschikbaar wordt gesteld
- De telewerker zelf

Deze schakels vindt men ook bij diensten, producten of taken binnen het burgerzakendomein. Voorbeelden van situaties zijn:

- Adresonderzoek in het veld zoals huisbezoeken.
- Loket voor aangifte geboorte in het ziekenhuis.
- Thuisbezorging van persoonsgegevens bevattende documenten, zoals paspoorten en rijbewijzen.
- Inschrijving van vluchtelingen in de BRP op een alternatieve locatie.
- Afgifte verlof tot lijkbezorging

- Gegevens bewerken thuis bij de medewerker Burgerzaken

Gedragsregels

Bij de gedragsregels gaat het vooral om bewustwording bij en bescherming van de telewerker. Een handtekening onder een verklaring biedt op zich nog geen waarborg voor de privacybescherming. Bepalend is hoe de telewerker feitelijk acteert. Dit vereist monitoring door de aansturende manager en periodiek aandacht voor en voorlichting over de risico's en regels.

I Eisen aan ruimte waarin wordt gewerkt
De gemeente bepaalt zelf welke telewerkplaatsen (dus buiten het gemeentekantoor) zijn toegestaan. Voorbeelden daarvan zijn: de eigen privéwoning, een ander kantoor waar werkzaamheden verricht worden waarbij persoonsgegevens geraadpleegd en/of bewerkt worden en buiten op locaties waar bij de uitvoering van werkzaamheden op dat moment persoonsgegevens nodig zijn. Het moet voor de telewerker volstrekt duidelijk zijn waar de grenzen liggen. De risicoanalyse kan goed helpen om de afbakening te maken.

Als de telewerker bijvoorbeeld thuis werkt, zijn er voorwaarden vastgesteld waaraan die thuislocatie moet voldoen en zijn er gedragsregels voorgeschreven. Hierbij kan gedacht worden aan het niet onbeheerd achterlaten van de werkplek terwijl het *apparaat* nog in verbinding staat met het gemeentelijke systeem. In het product Telewerkbeleid zijn duidelijke voorbeelden opgenomen van maatregelen die moeten worden genomen.[2]

II Eisen aan het apparaat waarmee wordt gewerkt

In het 'veldwerk' van burgerzaken is het vaak nodig om te kunnen raadplegen in de gegevensverzameling. Voorbeeld: De telewerker heeft buiten het gemeentekantoor gegevens nodig uit de BRP bij huisbezoeken in het kader van adresonderzoek. Hij kan gegevens over dat adres meenemen en beschikt er dan offline over, maar ook dan zijn er gevaren voor de privacy. Deze gegevens gaan over straat en kunnen verloren worden. Als de telewerker op het moment dat hij het nodig heeft een online verbinding tot stand brengt met het systeem waarin de gegevens zijn opgeslagen heeft hij een korte tijd de beschikking over actuele gegevens en na het huisbezoek verbreekt de verbinding automatisch na 30 seconden en gaat hij verder over straat zonder persoonsgegevens op zak.

Omgang met het apparaat
In het *apparaat* zijn geen persoonsgegevens opgeslagen.
De telewerker maakt verbinding met het gemeentelijke systeem op het moment dat hij gegevens nodig heeft. De fysieke omstandigheden waarin dat gebeurt worden door het gemeentelijk beleid ingekaderd. Bij het bepalen van dat kader speelt wederom de risicoanalyse een zeer behulpzame rol. De omgang met de toegangscodes en of andere mogelijke benodigdheden zoals een chipcards zijn vastgelegd in het gemeentelijke beleid en zijn verplicht.

Persoonlijk gebruik van apparaat en niet door derden
De toegang via het *apparaat* mag alleen gebruikt worden door de telewerker zelf, die daarvoor geautoriseerd is.

In beginsel geen persoonsgegevens printen of kopiëren
De telewerker wordt verboden om geraadpleegde gegevens uit te printen of anderszins te kopiëren

[2] Pagina 9 Telewerkbeleid gemeente v 1.0

en op een andere plek op te slaan tenzij het formeel vastgelegde werkproces waarin de gegevens gebruikt worden daar expliciet om vraagt. Het is dus niet ad hoc ter beoordeling van de individuele medewerker. Het is dus zaak dat het vastgelegde werkproces gebruikt kan worden om dit soort situaties af te vangen.

III Af te leggen verklaring vóór ingebruikname toegangsmogelijkheid
De functies waarbij telewerken onderdeel is, kunnen alleen vervuld worden door personen die de verklaring hebben afgelegd en getekend en voldoende gescreend zijn. (denk aan een VOG of C screening[3])

De telewerker wordt gevraagd een verklaring te ondertekenen alvorens hij de technische mogelijkheid krijgt van toegang tot het gemeentelijke systeem. Onderdelen van de verklaring zijn in ieder geval:

- Geheimhoudingsverklaring
  De persoonsgegevens waar hij kennis van krijgt, houdt hij geheim en speelt hij niet door aan derden, tenzij dit geregeld is in de vastgestelde procesbeschrijvingen.
- Integriteitverklaring
  Hij verklaart de gegevens alleen te gebruiken voor de hem opgelegde taken en geenszins voor eigen persoonlijk belang.
- Gedragscode
  Hij verklaart zich te conformeren aan de regels die zijn vastgelegd in de gedragscode die voor telewerkers geldt.

Bewerken van gegevens

Bij het bewerken van persoonsgegevens, zijn in de regel bronnen nodig waaraan nieuw aan te brengen gegevens te ontlenen zijn[4]. Het beleid geeft aan dat deze bronnen slechts te gebruiken zijn indien zij via inlog in een systeem van de gemeente te benaderen zijn. Daarmee wordt uitgesloten dat papieren informatiedragers voor de bewerking het gemeentekantoor mogen verlaten.

Uitgangspunten en voorwaarden bij autorisatie

Om überhaupt te kunnen werken met persoonsgegevens is autorisatie nodig. De autorisatie geeft aan of bepaalde functionaliteiten en gegevens gebruikt mogen worden binnen het plaatsonafhankelijk werken of dat dit alleen binnen de muren van het gemeentehuis of stadskantoor mag plaatvinden.

Te onderscheiden autorisaties zijn:

Autorisatie voor GBA-V
Voor een directie raadpleegmogelijkheid in de centrale verstrekkingsvoorziening van de BRP (dat heet nu nog GBA-V) is een autorisatie afgegeven door de minister van BZK. De Rijksdienst voor Identiteitsgegevens (RvIG) geeft hieraan uitvoering. Het betreft een standaardautorisatie die voor elke gemeente geldt en bedoeld is om uitvoering te geven aan een kleine 30 gemeentelijke taken die zijn genoemd in het autorisatiebesluit. Het besluit voorziet in de autorisatie van de gemeente als

[3] Onderzoek door AIVD die een Verklaring van Geen Bezwaar kan afgeven op basis van een veiligheidsonderzoek bij aanstellingen in vertrouwensfuncties.
[4] De bronnen voor de opname van BRP-gegevens zijn beschreven in de artikelen 2.8 t/m 2.25 Wet BRP.

bestuursorgaan.
Om een individuele gemeentemedewerker in staat te stellen om deze raadpleegfunctie te gebruiken is een nadere autorisatie van college van B&W zelf nodig. M.a.w. de gemeentelijke organisatie treft een voorziening om de mogelijkheid te effectueren. De individuele medewerker vervult een functie en heeft daarbinnen de rol die opgenomen is in de hierboven genoemde autorisatiematrix.

Autorisatie voor lokaal BRP-bestand
Gemeentemedewerkers kunnen ook geautoriseerd worden om direct te raadplegen in het lokale bestand van de BRP. Dit bestand is nu nog het oorspronkelijke bronbestand van de BRP voor wat betreft de eigen gemeente. De toegang moet geregeld zijn in een gemeentelijke verordening zoals bedoeld in artikel 3.8 Wet BRP.

Autorisatie voor gegevensmagazijn
Omdat het lokale BRP-bestand uiteindelijk zal verdwijnen zodra de gemeente overgaat op de nieuwe BRP-voorzieningen (vanaf medio 2018 kan dit zich gaan voordoen), zal het raadplegen van persoonsgegevens door individuele gemeentemedewerkers kunnen plaatsvinden in het gemeentelijke gegevensmagazijn. Autorisatie hiervoor is niet geregeld in de Wet BRP, maar zal de gemeente zelf moeten regelen in autorisatiebesluiten.

Uitgangspunten en voorwaarden t.a.v. techniek

- Van belang is dat helder moet zijn met welk *apparaat* de toegang verkregen kan worden, aan welke eisen dat *apparaat* moet voldoen.
- In het beleid wordt bijvoorbeeld de keuze gemaakt voor het gebruik van een *apparaat* dat door de gemeente aan de telewerker wordt verstrekt. Het is dan niet toegestaan of mogelijk dat met een ander (privé) *apparaat* wordt gewerkt bij het raadplegen van persoonsgegevens.
- De verbinding met het gemeentelijke systeem vindt plaats via een netwerk. Binnen de gemeente worden hiervoor een aantal technische eisen vastgesteld om te voorkomen dat onveilige netwerken worden gebruikt zoals openbare wifi-netwerken.
- Als de gemeente toestaat om met privé-apparatuur te werken dan mag dat alleen binnen een beveiligde netwerkomgeving gebeuren. Voorbeelden zijn: Werken met passcode; authenticatie van degene die inlogt.
- Via logging is steeds terug te halen wie verbinding heeft gemaakt met het gemeentelijk systeem, wanneer dat was en welke acties zijn uitgevoerd.
- Op het *apparaat* worden geen persoonsgegevens opgeslagen (‘zero footprint’). Ook niet op externe geheugenschijf of –chip.
- Externe bronnen en netwerken (zoals SUWI, RDW) worden geblokkeerd of begrensd volgens de besluiten die de gemeente hierover heeft genomen. Of blokkering of begrenzing noodzakelijk is, hangt af van het formeel vastgestelde werkproces.
- Binnen de autorisatiebesluiten is geregeld aan welke functies toegang wordt verleend en tot welke systemen. Er is een koppeling tussen functies en rollen (RBAC[5]). Deze staan in een autorisatiematrix welke de grondslag is voor het toekennen van toegang tot systemen en rollen binnen de burgerzakenapplicaties met bijbehorende rechten (inkijk- of mutatierechten).
- De aard van de verbinding wordt voorgeschreven (vast, draadloos, netwerk) en maatregelen worden getroffen tegen schadelijk software zoals virussen.

[5] Role-based access control is een methode waarmee op een effectieve en efficiënte wijze toegangscontrole voor informatiesystemen kan worden ingericht.

- Geregeld wordt dat er een vorm is van schermbeveiliging en dat het *apparaat* automatisch uitlogt na inactiviteit van 5 minuten. Ook bij het verlaten van de werkplek dient het *apparaat* vergrendeld te worden.

Bijlage 1:

Telewerkbeleid gemeente van IBD (BIG)

Bijlage 2:

Voorbeeld van documenten die plaatsonafhankelijk bewerken en raadplegen van persoonsgegevens ondersteunen

Voorstel aan het MT

Onderwerp toegang tot de BRP bij thuiswerken door medewerkers Burgerzaken

Afdeling Burgerzaken

Datum ….

Korte omschrijving / kern van het voorstel

In het kader van de voorbereiding op 'het nieuwe werken' is er een groeiende behoefte bij Burgerzaken om thuis te werken. Voor de werkzaamheden is het voor een aantal medewerkers Burgerzaken van essentieel belang dat kan worden beschikt over de BRP. Het gaat dan niet alleen om raadplegen van gegevens maar ook het uitvoeren van mutaties en controles en het afwerken van het GBA-berichtenverkeer.

Met een token is het technisch mogelijk toegang te krijgen tot de burgerzakenapplicatie. De medewerker heeft dan dezelfde autorisaties als op de kantoorwerkplek. Het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties heeft eerder aangegeven dat het werken met persoonsgegevens buiten het gemeentehuis of stadskantoor onwenselijk is. Echter, het gebruik van deze persoonsgegevens binnen ' het nieuwe werken' is noodzakelijk. De medewerker moet basisgegevens kunnen gebruiken als hij thuis werkt. Anders zal 'het nieuwe werken' binnen Burgerzaken nauwelijks uitvoerbaar zijn.

De verbinding middels een token, waarmee thuis de verbinding wordt gemaakt, is beveiligd en heeft eenzelfde veiligheidsniveau als de verbinding op de werkplek binnen het stadskantoor. Wel moet de computer thuis voldoende beveiligd zijn. Daaraan wordt een aantal specifieke eisen gesteld. Het risico op misbruik wordt zeer gering geacht. Het gaat om een erg kleine groep medewerkers die bovendien jaren gewend zijn aan het werken met persoonsgegevens en de daarbij behorende privacy- en beveiligingsvoorschriften.

De medewerkers hebben behoefte aan een formele ambtelijke goedkeuring om op de thuiswerkplek gebruiken te mogen maken van de BRP. Pas dan zullen ze hiertoe over gaan.

Wat wordt concreet, in essentie van het MT gevraagd?

Formeel toegang te verlenen aan medewerkers van Burgerzaken om de BRP op hun thuiswerkplek te gebruiken, zodat zij ook op hun thuiswerkplek BRP-werkzaamheden kunnen verrichten, waarbij toegang tot de BRP essentieel is. Aan die toegang wordt een aantal voorwaarden verbonden op het terrein van techniek en gedrag.

Voorgesteld besluit

Het MT besluit:

1. Aan de specifiek aangewezen (of “specifiek aan te wijzen”)medewerkers Burgerzaken toestemming te verlenen om thuis de BRP te gebruiken voor raadplegen, muteren en corrigeren van persoonsgegevens en/of het afhandelen van het GBA-berichtenverkeer.
2. Toegang tot de BRP te beperken tot een werkplek in de eigen woning;
3. Aan de toegang tot de BRP de volgende aanvullende voorwaarden te verbinden:
   - Toegang tot de BRP wordt tot stand gebracht middels een token met ID-code, waarmee een beveiligde verbinding tot stand wordt gebracht.
   - De thuiswerkplek is voorzien van deugdelijke en actuele antivirussoftware en beveiliging. Bij twijfel hierover wordt de functioneel applicatiebeheerder geraadpleegd en moeten zijn aanwijzingen worden opgevolgd.
   - Als de werkplek wordt verlaten en er andere mensen aanwezig zijn in de woning, wordt de BRP-applicatie afgesloten.
   - Er wordt niet meer ‘werkvoorraad’ meegenomen dan in één dag kan worden afgewerkt.

Aanvraag thuiswerken met de BRP

Ondergetekende,

1. Naam : _____|
2. functie : _____|
3. Personeels ID-nr : _____|

verzoekt toegang tot de BRP vanaf de thuiswerkplek voor raadplegen, muteren en corrigeren van persoonsgegevens en/of het afhandelen van het GBA-berichtenverkeer.
Betrokkene verklaart daarvoor zich aan de volgende (gedrags)regels te houden:

- Gebruik van de BRP wordt buiten het kantoor alleen toegestaan op een werkplek in de eigen woning.
- Toegang tot de BRP wordt tot stand gebracht middels een token met ID-code, waarmee een beveiligde verbinding tot stand wordt gebracht.
- De thuiswerkplek maakt gebruik van een legale versie van een besturingssysteem (bijv. Windows XP, 7 of 8) en applicaties (zoals Word, Excel, etc.)
- De thuiswerkplek is voorzien van een up-to-date virusscanner. Bij twijfel hierover wordt de functioneel applicatiebeheerder geraadpleegd en moeten zijn aanwijzingen worden opgevolgd.
- De thuiswerkplek is beveiligd op basis van een wachtwoord en de beveiliging (lock computer) wordt automatisch na 5 minuten standby geactiveerd.
- Als de werkplek wordt verlaten en er andere mensen aanwezig zijn in de woning, wordt de burgerzakenapplicatie afgesloten.
- Er wordt niet meer ‘werkvoorraad’ meegenomen dan in één dag kan worden afgewerkt.

Bovenstaande regels vormen een aanvulling op die, die bij de autorisatie voor de BRP horen (privacy, terugmelding, wachtwoordgebruik, etc.).

Datum : ___| - ___| - _____| Handtekening : _____|

Akkoord afdelingshoofd

Datum : ___| - ___| - _____| Handtekening : _____|

Aanvraag autorisatie raadplegen, muteren en corrigeren BRP

IN TE VULLEN DOOR AANVRAGER

Naam : _____|

Functie : _____|

Personeels ID-nr : _____|

Datum einde dienst: ___| - ___| - _____|

Aanvrager verklaart bekend te zijn met de hieronder vermelde regels over het gebruik van de raadpleegfunctie BRP-gegevens en de verplichtingen na te leven die daarin zijn vermeld.

Gebruik van de raadpleegfunctie

- Geautoriseerden hebben een geheimhoudingsplicht t.a.v. de aan hen toegekende gebruikersidentificaties en wachtwoorden.
- De wachtwoorden worden eens in de 90 dagen gewijzigd.
- Het systeem controleert of het wachtwoord verschilt met het voorgaande wachtwoord.
- De geautoriseerde wordt geblokkeerd nadat driemaal een foutief wachtwoord is ingegeven.
- Van de blokkering wordt door het systeem melding gemaakt.
- Bij functiewijziging van een geautoriseerde dienen de toegekende gebruikers-identificaties te vervallen
- Het werkstation van de raadpleegfunctie wordt zodanig opgesteld dat derden geen kennis kunnen nemen van de daarop gepresenteerde gegevens.
- De verbinding tussen het centrale computersysteem en het werkstation van de raadpleegfunctie dient gedurende de tijd dat deze niet wordt gebruikt te zijn afgesloten.
- Geautoriseerden van de raadpleegfunctie dienen vooraf van deze regeling in kennis te worden gesteld.
- Als geraadpleegde gegevens afwijking vertonen of niet in overeenstemming zijn met de geconstateerde werkelijkheid, is de geautoriseerde verplicht dit terug te koppelen naar de gegevensbeheerder BRP.

Privacyaspecten

- De mogelijkheid tot het raadplegen van gegevens uit de BRP wordt beperkt tot gegevens die de geautoriseerde uitsluitend voor zijn/haar taakvervulling nodig heeft.
- De raadpleegfunctie mag uitsluitend voor de eigen bedrijfsvoering van de gemeente worden gebruikt. Het is niet toegestaan gegevens hieruit aan derden te verstrekken.
- De geautoriseerden hebben ten aanzien van het gebruik van de raadpleegfunctie van de BRP een geheimhoudingsplicht ten aanzien van de gegevens die zij uit de BRP raadplegen of hebben geraadpleegd.
- Gegevens van personen uit de BRP dienen na gebruik zorgvuldig te worden vernietigd. Dit dient zodanig te geschieden dat hierop voorkomende gegevens niet meer herleidbaar zijn naar ingeschreven personen.
- Van de aanvragen tot toegang en/of verwijdering van de raadpleegfuncties wordt door de applicatiebeheerder een administratie bijgehouden.

- Van de verstrekte autorisaties wordt een aantekening geplaatst in het gemeentelijke personeelsbestand. Hieruit wordt informatie verstrekt aan de applicatiebeheerder over wijziging van de functie / afdeling van de geautoriseerde of beëindiging van het gemeentelijk dienstverband.

Incidentmelding
Elke medewerker van de gemeente (zowel intern als extern) is verplicht een beveiligingsincident te melden aan de gegevensbeheerder BRP. De medewerkers zijn eveneens verplicht zwakke plekken in de beveiliging en in de programmatuur te melden. Deze verplichting is erop gericht tekortkomingen in de beveiliging van de apparatuur en programmatuur en de omgang daarmee zo snel mogelijk te ontdekken en te kunnen oplossen.

Logging
De handelingen van de geautoriseerden worden gelogd.

Datum : ___| - ___| - _____| Handtekening : _____|

IN TE VULLEN DOOR LEIDINGGEVENDE

Naam : _____|

Functie : _____|

Telefoon : _____|

Aanvrager verricht werkzaamheden ten behoeve van de bijhouding van de BRP en dient daarvoor over de volgende functionaliteiten van de burgerzakenapplicatie te beschikken:

☐ Raadplegen personen
☐ Muteren personen
☐ Corrigeren personen
☐ Burgerlijke Stand Module
☐ Raadplegen panden
☐ Muteren panden
☐ Corrigeren panden
☐

Datum : ___| - ___| - _____| Handtekening : _____|

IN TE VULLEN DOOR BURGERZAKEN

Voor akkoord privacybeheerder

Datum : ___| - ___| - _____|

Paraaf : _____|

voor akkoord functioneel beheerder

Datum : ___| - ___| - _____|

Paraaf : _____|