gemeente Oisterwijk

GEMEENTEBLAD

Officiële uitgave van de gemeente Oisterwijk

Nr. 192515

10 september 2018

BRP Beleid voor gebruik BRP buiten gemeentehuis

1. Inleiding
De Basis Registratie Personen (BRP) is de centrale registratie waarin alle persoonsgegevens van burgers (binnengemeentelijk) staan en worden bijgehouden. Deze basisregistratie staat totdat de modernisering van de BRP een feit is, voorlopig lokaal (binnen de gemeenten) dus in de eigen ICT infrastructuur. Mutaties in de BRP worden via berichtenverkeer uitgewisseld naar de landelijke voorziening.

2. Doelstelling
Gegevens uit de BRP zijn vertrouwelijk en kwetsbaar, daarom moet de beschikbaarheid, integriteit en vertrouwelijkheid altijd gewaarborgd zijn. De informatieveiligheid van de BRP gegevens zou ook extern (buiten het gemeentehuis) gewaarborgd moeten blijven.

3. Implementatie
Voor toegang op afstand (van buiten het gemeentehuis) tot de informatievoorziening gelden algemene beleid -en spelregels. Verder zijn er voor interne en externe medewerkers organisatie brede waarborgen rondom integriteit, geheimhouding en vertrouwelijkheid.
Gegevens uit de BRP hebben de hoogste classificatie op het gebied van informatieveiligheid. Daarom zijn er extra afspraken en maatregelen rondom deze gegevens en processen. De afspraken en maatregelen voor het gebruik en beheer buiten het gemeentehuis zijn in dit document beschreven.

4. Beleid
Oisterwijk hanteert de onderstaande beleidsuitgangspunten in het beleid voor het gebruik van mobiele apparatuur en deze zijn ontleend aan de Baseline Informatiebeveiliging Gemeenten (BIG).

• BRP gegevens worden gemuteerd in de basisregistratie. Muteren gaat via de applicatie Key2Burgerzaken.
• Slechts een beperkte groep medewerkers heeft buiten het gemeentehuis toegang tot de applicatie Key2Burgerzaken waarin de BRP gegevens worden geraadpleegd en gemuteerd. Zie hiervoor de bijlage.
• Voor overige collega's is Key2Burgerzaken in de thuiswerkomgeving NIET beschikbaar.
• Overige medewerkers kunnen via andere applicaties slechts beperkte persoonsgegevens uit de BRP raadplegen. Denk hierbij aan Corsa. Deze applicaties zijn via de thuiswerkomgeving beschikbaar. Deze thuiswerkomgeving bevat veiligheidswaarborgen zoals authenticatie, en veilige (internet)verbindingen. Voor de gekoppelde systemen geldt dat slechts een beperkte set met BRP gegevens beschikbaar is in deze applicaties. Deze set is uitgewerkt in de verordening BRP en de beheerregeling BRP.
• Daarnaast is er nog het landelijk stelsel voor de BRP. Dit is het GBA-V netwerk waarop alle overheidsinstanties die gebruik mogen maken van deze gegevens zijn aangesloten. Toegang tot het GBA-V netwerk is lokaal en onder verantwoording van hoofd afdeling Dienstverlening geregeld
• Voor de medewerkers die buiten het gemeentehuis wel rechtstreeks toegang hebben tot Key2Burgerzaken gelden bijzondere afspraken
Thuiswerkomgeving:
o Authenticatie via token met pincode en wachtwoord;
o Netwerk (internet)-verbinding via een beveiligde website (https);
o Inloggen op de netwerkomgeving met gebruikersnaam wachtwoord;
o Inloggen in de BRP applicatie met gebruikersnaam en wachtwoord;
o Thuiswerkplek is de privé omgeving van de medewerker (thuis);
o De interne waarborgen gelden in de thuiswerkomgeving ook (schermbeveiliging, antivirusbescherming);
o Ingelogde thuiswerkplek niet onbeheerd achter laten (ook niet voor gezin of familieleden);
o BRP gegevens zijn vertrouwelijk, voor derden (niemand kijkt mee);
o Vertrouwelijke documenten niet laten slingeren en na het afdrukken en gebruik veilig opbergen of vernietigen

Omtrent de applicatie Centric:
• Alleen toegang op initiatief gemeente (op aangeven van apllicatiebeheerder Key2Burgerzaken);
• Toegang vanuit kantoor leverancier;
• Authenticatie van de externe medewerker
• Authenticatie via remote sessie met leverancier;
• Netwerk (internet)-verbinding via een versleutelde verbinding (IPsec VPN)
• Inloggen op de netwerkomgeving met gebruikersnaam en wachtwoord;
• Inloggen in de BRP applicatie met tweeweg authenticatie

• Toegang en werken onder toezicht en verantwoording van eigen medewerker;

Voor de medewerkers specifiek van de afdeling Dienstverlening die thuiswerken:
• Netwerkverbinding via een IPsec VPN;
• Inloggen op de netwerkomgeving met gebruikersnaam wachtwoord met token
• Eventueel inloggen in de applicatie Key2Burgerzaken met gebruikersnaam en wachtwoord;
• De interne waarborgen gelden (schermbeveiliging, antivirusbescherming) ook thuis;
• Ingelogde werkplek niet onbeheerd achter laten; (uitloggen of werkstation vergrendelen);
• BRP gegevens zijn vertrouwelijk voor derden (niemand kijkt mee);
• Vertrouwelijke documenten niet laten slingeren en na het afdrukken en gebruik veilig opbergen of vernietigen.

Dit beleid treedt in werking na vaststelling door het College van B&W. Hiermee komt het oude beleid van de gemeente Oisterwijk te vervallen.

Aldus vastgesteld door het College van B&W van de gemeente,
De heer drs. J.F.M. Janssen, burgemeester
Mevrouw A.M.M. Depmann, gemeentesecretaris

Bijlage 1
Onderstaande medewerkers/rollen hebben rechtstreekse toegang tot Key2Burgerzaken buiten het gemeentehuis:

Proces	Wie	Waarom
Applicatie/gegevensbeheer	apllicatiebeheerder Key2Burgerzaken	Gegevensbeheer, verbetering kwaliteit van de persoonsgegevens.
Technisch applicatiebeheer	Corsa Beheer op afstand, verhelpen van verstoringen aan de applicatie Geen inhoudelijke mutaties aan BRP gegevens!	
Gegevensverwerking	Medewerkers de afdeling Dienstverlening	Dienstverlening dicht bij de burger