REGIO
RIJK VAN
NIJMEGEN

Privacybeleid Modulaire Gemeenschappelijke regeling Rijk van Nijmegen

Versie maart 2019

1. Inleiding

De Modulaire Gemeenschappelijke Regeling Rijk van Nijmegen (hierna: MGR) bestaat uit twee modules: het Werkbedrijf en iRvN. De iRvN levert ICT diensten aan de gemeenten die onderdeel uitmaken van de MGR. De iRvN heeft geen zeggenschap over de gegevens die zij voorbij ziet komen bij de uitvoering van haar dienstverlening. Daarom wordt de iRvN gezien als verwerker van de gegevens in het kader van de Algemene Verordening Gegevensbescherming (AVG). Het Werkbedrijf voert voor de diverse gemeenten taken uit in het kader van de Participatiewet, RMC, WMO en Wet sociale werkvoorziening (Wet sw). Het Werkbedrijf is (mede) verantwoordelijk voor de persoonsgegevens die zij verzamelt.

Binnen de MGR wordt veel gewerkt met persoonsgegevens van medewerkers, kandidaten en ondernemers. We verzamelen persoonsgegevens voornamelijk om onze wettelijke taken goed uit te kunnen voeren. Dit privacybeleid borgt dat we alles doen wat er in redelijkheid van ons verwacht mag worden om de privacy van kandidaten, ondernemers, medewerkers en andere betrokkenen te waarborgen, te beschermen en te handhaven.

Het privacybeleid is van toepassing op de gehele organisatie, alle processen, onderdelen, objecten en gegevensverzamelingen van de MGR. Dit beleid is in lijn met het algemene beleid van de MGR en de relevante lokale, regionale, nationale en Europese wet- en regelgeving.

Wettelijke kaders voor de omgang met persoonsgegevens
De MGR is verantwoordelijk voor het opstellen, uitvoeren en handhaven van het privacybeleid. Hiervoor is dit beleid in lijn met, of sluit aan op de actualiteiten van:

- Algemene Verordening Gegevensbescherming (AVG)
- Uitvoeringswet Algemene Verordening Gegevensbescherming
- Informatiebeveiligingsbeleid, vastgesteld door de MGR
- Code voor Informatiebeveiliging (NEN/ISO27002)
- Baseline Informatiebeveiliging Gemeenten / Baseline Informatiebeveiliging Overheden
- Participatiewet
- Wet Suwi
- WMO
- Wet sw
- Ambtenarenwet
- Archiefwet

Functionaris voor gegevensbescherming (FG)
De Functionaris voor gegevensbescherming is verantwoordelijk voor het intern onafhankelijk toezicht op en adviseren van de organisatie over de juiste en zorgvuldige omgang met persoonsgegevens. Hierbij kan de Functionaris voor gegevensbescherming rechtstreeks de Autoriteit Persoonsgegevens inschakelen.

Toezicht informatiebeveiligingsbeleid (CISO)
Gegevensbescherming kan niet geborgd worden zonder adequate informatiebeveiliging. Voor onafhankelijk toezicht op de uitvoering van het informatiebeveiligingsbeleid heeft het Dagelijks Bestuur een Chief Information Security Officer (CISO) aangesteld. De CISO is verantwoordelijk voor de organisatie van het informatiebeveiligingsbeleid. De FG en CISO informeren en consulteren elkaar over alle aspecten die van enig belang zijn voor de privacy.

Definities

Betrokkene: De persoon op wie de persoonsgegevens betrekking hebben. De betrokkene is degene van wie de gegevens worden verwerkt.

Persoonsgegevens: Alle gegevens die gaan over mensen en waaraan je een mens als individu kunt herkennen. Het gaat hierbij niet alleen om vertrouwelijke gegevens, zoals over iemands gezondheid, maar om ieder gegeven dat te herleiden is tot een bepaald persoon (bijvoorbeeld; naam, adres, geboortedatum). Naast gewone persoonsgegevens kent de wet ook bijzondere persoonsgegevens. Dit zijn gegevens die gaan over gevoelige onderwerpen, zoals etnische achtergrond, politieke voorkeuren of het Burgerservicenummer (BSN).

Verwerking: Een verwerking is alles wat je met een persoonsgegeven doet, al dan niet geautomatiseerd. Onder de AVG wordt daaronder begrepen:

- Verzamelen, vastleggen en ordenen;
- Bewaren, bijwerken en wijzigen;
- Opvragen, raadplegen, gebruiken;
- Verstrekken door middel van doorzending;
- Verspreiding of enige andere vorm van ter beschikkingstellen;
- Samenbrengen, met elkaar in verband brengen;
- Afschermen, uitwissen of vernietigen van gegevens.

Verwerkingsverantwoordelijke: Een persoon of instantie die alleen, of samen met een ander, het doel en de middelen voor de verwerking van persoonsgegevens vaststelt.

Verwerker: De persoon of organisatie die de persoonsgegevens verwerkt in opdracht van een andere persoon of organisatie.

2. Uitgangspunten

De MGR gaat op een veilige manier met persoonsgegevens om en respecteert de privacy van betrokkenen. De MGR houdt zich hierbij aan de volgende uitgangspunten.

Rechtmatigheid, behoorlijkheid
Persoonsgegevens worden in overeenstemming met de wet en op een behoorlijke en zorgvuldige wijze verwerkt.

Grondslag en doelbinding
De MGR zorgt ervoor dat persoonsgegevens alleen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doelen worden verzameld en verwerkt. Persoonsgegevens worden alleen met een rechtvaardige grondslag verwerkt.

Dataminimalisatie
De MGR verwerkt alleen de persoonsgegevens die minimaal noodzakelijk zijn voor het vooraf bepaalde doel. Waar mogelijk worden minder of geen persoonsgegevens verwerkt.

Persoonsgegevens moeten juist zijn
Het verwerken van onjuiste persoonsgegevens kan tot grote problemen leiden en een inbreuk vormen op de persoonlijke levenssfeer. De MGR draagt er zorg voor dat persoonsgegevens zorgvuldig en juist worden vastgelegd. Indien nodig neemt de MGR maatregelen om onjuiste verwerkingen te wissen of te rectificeren. De MGR heeft een actieve onderzoeksplicht als het aankomt op de juistheid van persoonsgegevens. Waar nodig dient de MGR de gegevens te actualiseren.

Integriteit en vertrouwelijkheid
De MGR gaat op een veilige, professionele en integere wijze met persoonsgegevens om. De privacy van betrokkenen wordt gerespecteerd. Zo worden persoonsgegevens alleen verwerkt door personen met een geheimhoudingsplicht en voor het doel waarvoor deze gegevens zijn verzameld. Daarbij zorgt de MGR

voor passende beveiliging van persoonsgegevens. Deze beveiliging is vastgelegd in het informatiebeveiligingsbeleid van de MGR.

Delen met derden
In het geval van samenwerking met externe partijen, waarbij sprake is van gegevensverwerking van persoonsgegevens, maakt de MGR afspraken over de eisen waar gegevensuitwisseling aan moet voldoen. Deze afspraken voldoen aan de wet. De MGR controleert deze afspraken. De MGR deelt in ieder geval maar niet uitsluitend gegevens met de bij de MGR aangesloten gemeenten, het UWV, de Belastingdienst, haar accountant, sociale ketenpartners (zoals Pluryn en Driestroom), het Zorg en Veiligheidshuis en met externe bedrijven die onze medewerkers inhuren of onze kandidaten in dienst (willen) nemen. Alleen de voor de dienstverlening noodzakelijke informatie wordt gedeeld.

Daarnaast kan de MGR met toestemming van een betrokkene informatie delen met een derde, zoals bijvoorbeeld een sociaal wijkteam.

Proportionaliteit en subsidiariteit
De inbreuk op de belangen van de betrokkene mag niet onevenredig zijn in verhouding tot de verwerking van persoonsgegevens voor het te dienen doel. Indien het doel waarvoor persoonsgegevens worden verwerkt op een minder nadelige wijze voor de betrokkene kan worden verwezenlijkt, dan kiest de MGR altijd voor die mogelijkheid.

Bewaartermijnen
Persoonsgegevens worden niet langer bewaard dan nodig is. Persoonsgegevens worden bewaard zolang ze van belang zijn voor het doel waarvoor ze zijn verzameld. De MGR heeft conform de Archiefwet de termijnen vastgelegd voor het bewaren van persoonsgegevens.

Sommige persoonsgegevens worden blijvend gearchiveerd voor historisch onderzoek of statistische doeleinden.

Doorgifte
De MGR geeft persoonsgegevens door aan de ESF ten behoeve van subsidies. De MGR deelt geen persoonsgegevens met een land buiten de Europese Economische Ruimte (EER), of een internationale organisatie.

Datalekken
We spreken van een datalek wanneer persoonsgegevens in handen vallen van derden die geen toegang tot die gegevens mogen hebben, of wanneer er een grote mate van waarschijnlijkheid is dat de gegevens in handen vallen van derden, bijvoorbeeld door het verlies van een bedrijfstelefoon of USB-stick. Wanneer er een datalek heeft plaatsgevonden moet de MGR dit zonder onredelijke vertraging, uiterlijk 72 uur nadat er kennis van de inbreuk is vernomen, aan het AP melden. Van onze medewerkers wordt verwacht dat zij een (mogelijk) datalek binnen 24 uur melden aan de CISO.

Het kan zijn dat de inbreuk een hoog risico met zich meebrengt voor de rechten en vrijheden van de betrokkenen. In dit geval meldt de MGR dit aan de betrokkenen in eenvoudige en duidelijke taal. Om toekomstige datalekken te voorkomen worden bestaande datalekken geëvalueerd.

3. Doeleinden en rechtmatige grondslag

Volgens de wet mogen persoonsgegevens alleen verzameld worden als daarvoor een doel is vastgesteld. Het doel moet uitdrukkelijk omschreven en gerechtvaardigd zijn. De gegevens mogen niet voor andere doelen verwerkt worden. Voor de uitvoering van sommige wetten, zoals bijvoorbeeld de Participatiewet, zijn de doelen voor het verwerken in de wet al vastgelegd.

De AVG bepaalt dat er voor elke verwerking van persoonsgegevens een rechtmatige grondslag uit de wet van toepassing moet zijn. Dat betekent dat de verwerking alleen mag plaatsvinden:

- Om een verplichting na te komen die in de wet staat
- Voor de uitvoering van een overeenkomst waar betrokkene partij van is
- Om een ernstige bedreiging voor de gezondheid van de betrokkene te bestrijden
- Voor de goede vervulling van een door de MGR uit te voeren taak
- Wanneer betrokkene toestemming heeft gegeven voor de specifieke verwerking

Vrijwel alle verwerkingen van persoonsgegevens door de MGR zijn gebaseerd op de uitvoering van een taak van algemeen belang, voortvloeiende uit de Participatiewet, WMO en Wet sw. De verwerkingen zijn dan nodig om onze medewerkers en kandidaten zo goed als mogelijk te kunnen bemiddelen naar passend werk. Daarnaast verwerkt de MGR gegevens op basis van een overeenkomst, te denken aan de arbeidsovereenkomst van onze ambtelijke medewerkers en SW medewerkers. Een derde veelvoorkomende rechtsgrondslag is de wettelijke verplichting waaraan wij moeten voldoen. Een voorbeeld hiervan is het verstrekken van loongegevens van onze medewerkers aan de fiscus of het UWV.

Afhankelijkheidsrelatie
Bij de uitvoering van publiekrechtelijke taken in het sociaal domein is er vrijwel altijd sprake van een afhankelijkheidsrelatie tussen de betrokkenen en de MGR. Zodra het weigeren van toestemming voor een verwerking gevolgen kan hebben voor een voorziening of de arbeidsrelatie, bijvoorbeeld het beëindigen van de dienstverlening of opleggen van een disciplinaire maatregel, is er sprake van een afhankelijkheidsrelatie. Het heeft in dat geval geen zin om toestemming te vragen, aangezien de toestemming ingetrokken kan worden en bovendien aangenomen kan worden dat de toestemming niet vrijelijk gegeven is. Slechts in uitzonderlijke gevallen is een toestemming nodig en heeft het zin deze te vragen, bijvoorbeeld als de MGR foto's van een persoon voor marketing doeleinden wil plaatsen op haar website e.d. Een ander voorbeeld betreft het delen van informatie met Wijkcentra of andere derde partijen met de uitdrukkelijke toestemming van betrokkene, mits het weigeren van toestemming niet tot negatieve gevolgen voor betrokken kan leiden.

4. Verwerking van persoonsgegevens

Wijze van verwerking
De hoofdregel van de verwerking van persoonsgegevens is dat het alleen toegestaan is in overeenstemming met de wet, en op een zorgvuldige wijze. Persoonsgegevens worden zoveel mogelijk verzameld bij de betrokkene zelf. De MGR voert verschillende wetten uit voor de aangesloten gemeenten, via mandaat of delegatie. De gemeenten en de MGR wisselen daarom ook veel gegevens met elkaar uit, voor zover nodig en toegestaan op grond van de toepasselijke wetgeving. Een voorbeeld daarvan is als een kandidaat op grond van de Participatiewet aangemeld wordt bij de MGR.

De MGR volgt bij de verwerking van persoonsgegevens de onder punt 2 genoemde uitgangspunten.

Beveiliging van persoonsgegevens
De MGR beveiligt alle persoonsgegevens. Dit moet voorkomen dat de persoonsgegevens kunnen worden ingezien of gewijzigd door iemand die daar geen recht toe heeft. Hoe de MGR dit doet staat in het informatiebeveiligingsbeleid van de MGR.

Algemene persoonsgegevens
Voorbeelden van algemene persoonsgegevens die de MGR verwerkt zijn:

- Voor- en achternaam
- Geslacht
- Geboortedatum

- Geboorteplaats
- Adresgegevens
- Telefoonnummer
- Emailadressen
- Salarisgegevens
- Gegevens over het functioneren (personeelsdossiers)

BSN en identiteitsbewijzen

Identiteitsbewijzen

De MGR is als werkgever (zowel ambtelijk als SW) verplicht om een kopie/scan van het identiteitsbewijs op te nemen voor de loonadministratie (art. 28 Wet op Loonbelasting). Het doel daarvan is aantonen dat de werknemer zich juist heeft gelegitimeerd en legaal in Nederland verblijft.

Ingeleend personeel moet geïdentificeerd worden bij aanvang van de tewerkstelling, maar er worden geen kopieën gemaakt of bewaard door de MGR. Alleen de noodzakelijke gegevens worden overgenomen en vastgelegd in de administratie.

Van kandidaten (Participatiewet en WMO) worden wel kopieën van paspoorten gemaakt en bewaard. Een kandidaat kan ervoor kiezen om op de kopie te schrijven. Alle persoonsgegevens (zoals de foto en het BSN) op de beschreven kopie moeten leesbaar zijn. Ook de foto moet voldoende zichtbaar blijven om de kandidaat te kunnen identificeren. Dat wat op de kopie is geschreven mag dus geen afbreuk doen aan de identificerende functie van de kopie.

De MGR verstrekt geen (kopieën van) identiteitsbewijzen aan andere organisaties, ook niet aan potentiële werkgevers of inleners.

BSN

Als werkgever moet de MGR Burgerservicenummers (BSN) van haar eigen medewerkers vastleggen in de administratie. Dit is zo geregeld in de Wet op de Loonbelasting. Als overheidsorganisatie gebruikt de MGR BSN's voor de uitvoering van haar wettelijke taken. Uiteraard gebruiken we het alleen als het noodzakelijk is. Als iemand alleen informatie opvraagt, vragen we niet naar het BSN.

Organisaties buiten de overheid mogen het BSN van onze kandidaten alleen gebruiken als dit in een specifieke wet is bepaald. Zo moet de bedrijfsarts het BSN ontvangen van de MGR, wanneer onze medewerker of kandidaat aangemeld wordt voor re-integratie.

Externe werkgevers en inleners

Kandidaten die via ons in dienst treden bij een werkgeversorganisatie, dienen zich daar zelf te legitimeren. De werkgever bewaart een kopie van het identiteitsbewijs.

Medewerkers die door de MGR gedetacheerd worden bij een inlener, moeten zich daar legitimeren. De inlener neemt bepaalde gegevens over van de gedetacheerde medewerker, waaronder het BSN. Dit is nodig voor identificatie bij de belastingdienst om de risico's van inleners- of ketenaansprakelijkheid te beperken. Daarnaast heeft de inlener het BSN nodig om te controleren of de betrokken medewerker tot de doelgroep banenafspraak en quotum arbeidsbeperkten behoort.

Bijzondere en gevoelige persoonsgegevens

De MGR verwerkt ook bijzondere persoonsgegevens. Dit is onvermijdelijk vanwege de taakstelling van de MGR. De MGR verwerkt de bijzondere persoonsgegevens altijd op basis van de Participatiewet, Wet sociale werkvoorziening of WMO, en als de gegevens relevant zijn voor de bemiddeling naar arbeid.

Gezondheidsgegevens

De MGR verwerkt gezondheidsgegevens, wanneer dat noodzakelijk is voor de bemiddeling naar arbeid, ten behoeve van re-integratie of als er sprake is van een direct risico voor betrokkene.

Van de arbeidsongeschikte medewerkers wordt te allen tijde een re-integratiedossier bijgehouden. Dit dossier bevat documenten van de bedrijfsarts en stukken voor het UWV. Daarin staan in de regel geen medische gegevens, tenzij het verwerken van medische gegevens nodig is voor de beoordeling van een recht op loon. In schrijnende gevallen kan het namelijk noodzakelijk zijn om wel medische informatie op te nemen in het dossier. Bijvoorbeeld als een medewerker claimt niet te kunnen werken vanwege een gebroken been, maar vervolgens dansend in de kroeg wordt gezien. Er is dan gerede twijfel over de rechtmatigheid van een ziekmelding. Voor zover de werknemer wel kan werken maar beperkingen heeft voor het werk, mogen de beperkingen zelf wel vermeld worden.

De SW-indicatie van onze SW-medewerkers bevat veel informatie over de gezondheid van de betrokken persoon. Deze SW-indicatie wordt door de MGR opgeslagen en bewaard, aangezien deze nodig is voor de verantwoording van ontvangen subsidies en omdat het noodzakelijk is voor de bemiddeling naar passende arbeid. De MGR is immers verplicht rekening te houden met de in de SW-indicatie vermelde beperkingen. De privacy van de betrokkenen wordt gewaarborgd door de SW-indicaties ontoegankelijk te maken voor onbevoegden.

Strafrechtelijk verleden
In de regel verwerkt de MGR strafrechtelijke gegevens slechts in de volgende situaties.

- Omdat een medewerker in detentie geen recht heeft op loon, wordt de detentieperiode vastgelegd in het personeelsdossier.
- Het dossier van de Participatiewet kandidaat die niet beschikbaar is voor werk wegens detentie, wordt met die informatie teruggestuurd naar zijn woongemeente.
- Soms is er strafrechtelijke informatie opgenomen in de SW-indicatie.
- Ook worden er arbeidsovereenkomsten gesloten tussen de Pompekliniek, de betrokkene in kwestie en de MGR. De driepartijen overeenkomst wordt bewaard in het personeelsdossier.

Buiten voornoemde voorbeelden verwerkt de MGR geen strafrechtelijke gegevens, tenzij het verwerken daarvan noodzakelijk is voor het voorkomen van gevaar voor anderen of voor de bemiddeling en plaatsing in arbeid.

Etnische afkomst en religieuze opvattingen
Deze gegevens verwerkt de MGR niet, tenzij er sprake is van omstandigheden die bepalend zijn voor bemiddeling naar werk of het vaststellen van een recht op loon.

Lidmaatschap vakbond
De MGR verwerkt dit gegeven niet, tenzij verwerking daarvan noodzakelijk is voor het toekennen van (bijzonder) verlof en inherent daaraan de doorbetaling van loon.

Overige bijzondere persoonsgegevens
De AVG vermeldt ook andere bijzondere persoonsgegevens, zoals politieke opvattingen, lidmaatschap vakbond en seksuele geaardheid. De MGR verwerkt deze gegevens niet.

Gevoelige persoonsgegevens die geen bijzondere persoonsgegevens zijn
Onze doelgroepen uit de Wet sw, Participatiewet en WMO hebben veelal te maken met privé situaties of problematiek, welke van invloed kan zijn op bemiddeling naar arbeid of de toekenning van een voorziening. Soms wordt er informatie over de privé situatie vermeld in de SW-indicatie. Het gaat dan om heel gevoelige informatie, welke door de AVG niet aangemerkt wordt als een bijzonder persoonsgegeven. Daarbij kan het gaan om:

- Gegevens over de financiële of economische situatie van de betrokkenen, zoals schulden, salaris- en betalingsgegevens, werksituatie, arbeidsovereenkomsten, fraude constatering, maatregel oplegging en financiële redenen voor einde uitkering.
- (Andere) gegevens die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene, zoals gegevens over:

- Beschrijving (niveau/ernst/verwijtbaarheid) van gedrag, competenties, capaciteiten, vaardigheden en leerbaarheid.
- Beschrijving van persoonlijke/thuissituatie, multiprobleem situatie, verslaving, opname in tbs of justitiële jeugdinrichting.
- Prestaties op school, arbeidsverleden.

- Gegevens over kwetsbare groepen zoals minderjarigen, mensen die te maken hebben met stalking of mensen die in een blijf-van-mijn-lijfhuis verblijven.
- Gegevens van kinderen, mensen met een verstandelijke handicap en mensen die in aanmerking komen voor bemiddeling op grond van de Wet sw, WMO, Participatiewet en RMC.

Gevoelige persoonsgegevens worden uitsluitend verwerkt indien en voor zover dit nodig is voor de bemiddeling naar werk, of voor het vaststellen van een recht op loon. De gegevens worden zo spoedig mogelijk verwijderd als ze niet meer nodig zijn en de wettelijke bewaartermijn verstreken is.

5. Transparantie en communicatie

Informatieplicht (Artikel 13,14, AVG)
De MGR informeert betrokkenen over het verwerken van persoonsgegevens. Wanneer betrokkenen gegevens aan de MGR geven, worden zij op de hoogte gesteld van de manier waarop de MGR met persoonsgegevens om zal gaan. Dit kan bijvoorbeeld via een formulier gebeuren. Vaak staat op de aanvraagformulieren vermeld welke gegevens zonder toestemming niet openbaar gemaakt zullen worden. De betrokkene wordt niet nogmaals geïnformeerd als hij/zij al weet dat de MGR persoonsgegevens van hem/haar verzamelt en verwerkt, en weet waarom en voor welk doel dat gebeurt.

Wanneer de gegevens via een andere weg verkregen worden, dus buiten de betrokkene om, wordt de betrokkene geïnformeerd op het moment dat deze voor de eerste keer worden verwerkt.

Verwijdering
De MGR bewaart de persoonsgegevens niet langer dan nodig is voor de uitvoering van haar taken, of zoals vastgelegd in de Archiefwet. Wanneer er nog persoonsgegevens opgeslagen zijn die niet langer nodig zijn voor het bereiken van het doel, worden deze zo snel mogelijk verwijderd. Dit houdt in dat deze gegevens vernietigd worden, of zo worden aangepast dat de informatie niet meer gebruikt kan worden om iemand te identificeren.

Rechten van betrokkenen (Artikel 13 t/m 20, AVG)
De wet bepaalt niet alleen de plichten van degenen die de persoonsgegevens verwerken, maar bepaalt ook de rechten van de personen van wie de gegevens worden verwerkt. Deze rechten worden ook wel de rechten van betrokkenen genoemd, en bestaan uit de volgende rechten:

- Recht op informatie: Betrokkenen hebben het recht om aan de MGR te vragen of zijn/haar persoonsgegevens worden verwerkt.
- Inzagerecht: Betrokkenen hebben de mogelijkheid om te controleren of, en op welke manier, zijn/haar gegevens worden verwerkt.
- Correctierecht: Als duidelijk wordt dat de gegevens niet kloppen, kan de betrokkene een verzoek indienen bij de MGR om dit te corrigeren.
- Recht van verzet: Betrokkenen hebben het recht aan de MGR te vragen om hun persoonsgegevens niet meer te gebruiken.
- Recht om vergeten te worden: In gevallen waar de betrokkene toestemming heeft gegeven om gegevens te verwerken, heeft de betrokkene het recht om de persoonsgegevens te laten verwijderen.

- Recht op bezwaar: Betrokkenen hebben het recht om bezwaar aan te maken tegen de verwerking van zijn/haar persoonsgegevens. De MGR zal hieraan voldoen, tenzij er gerechtvaardigde gronden zijn voor de verwerking.

Indienen van verzoek
Om gebruik te maken van voornoemde rechten kan de betrokkene een verzoek indienen. Dit verzoek kan schriftelijk of via de e-mail ingediend worden. De MGR heeft vier weken de tijd, vanaf de ontvangst van het verzoek, om te beoordelen of het verzoek gerechtvaardigd is. Binnen vier weken zal de MGR laten weten wat er met het verzoek gaat gebeuren. Als het verzoek niet wordt opgevolgd is er de mogelijkheid om bezwaar te maken bij de MGR, of een klacht in te dienen bij de Autoriteit Persoonsgegevens (AP). Aan de hand van een verzoek kan de MGR aanvullende informatie opvragen om zeker te zijn van de identiteit van de betrokkene. In dat geval verschuift de periode van vier weken waarbinnen de MGR dient te reageren op het verzoek.

6. Cameratoezicht

Binnen de bedrijfspanden van de MGR wordt gebruik gemaakt van cameratoezicht. Cameratoezicht wordt onder andere gebruikt voor het vergroten van de veiligheid binnen de panden en op het parkeerterrein van de MGR. Camera's kunnen een grote inbreuk maken op de privacy van diegene die gefilmd worden. Om de privacy zo goed mogelijk te waarborgen worden camera's alleen ingezet wanneer er geen andere manieren zijn om het doel te bereiken, en worden er eisen gesteld aan de inzet van camera's.

7. iRvN

De iRvN is verwerker in het kader van de AVG en verzorgt in die hoedanigheid de verwerking van persoonsgegevens voor de gemeenten die zijn aangesloten bij het Rijk van Nijmegen en de module Werkbedrijf van de MGR. De iRvN streeft een zorgvuldige en veilige verwerking van gegevens na, conform de vereisten die eerder zijn verwoord in dit beleidsdocument en doet dit door zoveel mogelijk de tactische richtlijnen en normen te hanteren zoals vermeld in de landelijke *"Baseline Informatiebeveiliging Overheden"* (tot 2020 ook Baseline Informatiebeveiliging Gemeenten) zijn geformuleerd.

Om de privacyregels na te leven is zoveel mogelijk functiescheiding toegepast en worden autorisaties uitgegeven volgens het principe *"precies genoeg om het werk te kunnen doen"*. Voor veiligheidsincidenten die direct met de privacy gevoeligheid van gegevens te maken hebben wordt conform de voorschriften van de AVG gewerkt. Voor de afhandeling van datalekken is de al eerder genoemde speciale "datalek" procedure geïmplementeerd waarbij het wegnemen van de gevolgen voor betrokkene(n) en het herstellen van het lek de hoogste prioriteit heeft. Datalekken worden binnen de gestelde termijn gemeld aan de verantwoordelijke.

Ten slotte zijn naast de procedurele en organisatorische maatregelen alle belangrijke en moderne technische oplossingen geïmplementeerd, met als doel om misbruik van privacy gevoelige gegevens door hacks, phishing of ransomware aanvallen te weerstaan.