MAASDRIEL

GEMEENTEBLAD

Officiële uitgave van de gemeente Maasdriel

Nr. 177977

25 april

2023

Privacybeleid Bommelerwaard 2023 – 2026

1. Inleiding

De gemeente Maasdriel, gemeente Zaltbommel en de Bedrijfsvoeringseenheid Bommelerwaard (hierna: de organisaties) werken met (persoons)gegevens van onder andere burgers, ondernemers, medewerkers en (keten)partners. Deze persoonsgegevens verzamelen de organisaties om de gemeentelijke wettelijke taken en bedrijfsvoeringstaken goed uit te kunnen voeren. Denk hierbij aan taken in het sociaal domein, openbare orde, veiligheidsdomein en burgerzaken. Om deze taken goed uit te kunnen voeren is het noodzakelijk dat de organisaties persoonsgegevens verwerken. Personen op wie de persoonsgegevens betrekking hebben moeten erop kunnen vertrouwen dat de organisaties zorgvuldig en veilig met deze persoonsgegevens omgaan.

Nieuwe technologische ontwikkelingen, innovatieve voorzieningen, globalisering en een steeds meer digitaal wordende overheid maakt het zorgvuldig omgaan met persoonsgegevens steeds complexer. De organisaties zijn zich hiervan bewust en willen met dit beleid aangeven hoe zij in algemene zin invulling geven aan nationale en Europese wet- en regelgeving op het gebied van privacy, waaronder de Algemene Verordening Gegevensbescherming (hierna te noemen: AVG) en aanvullend voor de gemeente Maasdriel ook de Wet politiegegevens (hierna: Wpg).

Geldigheidsduur
Het beleid wordt tenminste eens per drie jaar beoordeeld en zo nodig herzien. Indien daar aanleiding toe is (bijvoorbeeld bij grote organisatorische veranderingen, wetswijzigingen, uitkomsten van DPIA's/GEB's) kan het college besluiten tot een tussentijdse herziening. Het beleid blijft onverminderd van kracht totdat een herzien beleid goedgekeurd wordt.

2. Begripsbepalingen

De definities van art. 4 AVG hebben in dit beleidsdocument dezelfde betekenis.

3. Visie

De komende jaren blijven de organisaties zich inzetten op het verhogen van de privacy bewustwording, de verdere professionalisering van de privacy functie in de organisaties en het verder verankeren van gegevensbescherming in het kader van privacy binnen de processen. Een goede privacy administratie is noodzakelijk voor het goed functioneren van de organisaties en is de basis voor het beschermen van rechten van personen. Dit vereist een integrale aanpak, goed eigenaarschap en risicobewustzijn. Ieder organisatieonderdeel is hierbij betrokken. Het is essentieel voor gegevensbescherming binnen de organisaties dat alle medewerkers zich verantwoord en bewust gedragen.

4. Doel

Met dit privacybeleid geven de organisaties een kader voor het verantwoord omgaan met persoonsgegevens en het waarborgen van de persoonlijke levenssfeer in relatie tot de verwerking van persoonsgegevens. Daarnaast beoogt dit privacybeleid de rollen, taken en verantwoordelijkheden op het gebied van de bescherming van persoonsgegevens helder af te bakenen.

De verdere uitwerking van dit beleid is - waar relevant - vastgelegd in de operationele documenten binnen de organisaties, zoals handreikingen, gedragscodes, concrete werkprocedures of werkafspraken voor algemene onderwerpen zoals datalekken, maar ook domeinspecifieke onderwerpen als gegevensdeling voor de uitvoering van de Jeugdwet of de Wet Maatschappelijke Ondersteuning.

Naast, het door de colleges van de gemeenten en bestuur van de bedrijfsvoeringseenheid vastgestelde privacybeleid, is een informatiebeveiligingsbeleid vastgesteld. Hierin zijn maatregelen opgenomen om de beschikbaarheid, integriteit en vertrouwelijkheid van (persoons)gegevens te garanderen. Informatiebeveiliging is een randvoorwaarde voor de bescherming van persoonsgegevens. Het gemeentelijke privacybeleid kan daarom niet los worden gezien van het gemeentelijke informatiebeveiligingsbeleid.

Verantwoordelijkheid van iedere medewerker
Alle medewerkers zijn verantwoordelijk voor het zorgvuldig omgaan met persoonsgegevens. De organisaties verlangen van al haar medewerkers en alle personen die werkzaam zijn voor de organisaties, zoals inhuurkrachten, dat de voorschriften van dit privacybeleid worden opgevolgd en actief worden uitgedragen.

5. Reikwijdte

De organisaties verzamelen en gebruiken persoonsgegevens van inwoners, leveranciers en medewerkers en andere natuurlijke personen (hierna te noemen: betrokkenen).

Dit privacybeleid is van toepassing op alle verwerkingen van persoonsgegevens door of namens de organisaties, waaronder:
1. De verwerking van persoonsgegevens binnen de bedrijfsprocessen van de organisaties;
2. De verwerking van persoonsgegevens die is uitbesteed, of op een andere manier is georganiseerd, zoals deelname van de organisaties aan een rechtspersoon die voor de organisaties bepaalde diensten verricht;
3. De gegevensuitwisseling met derde partijen zoals bij samenwerkingsverbanden of leveranciers.

6. Principes voor de verwerking van persoonsgegevens

De AVG is gebaseerd op een aantal principes voor de verwerking van persoonsgegevens. De organisaties onderschrijven deze principes en stellen zich ten doel persoonsgegevens te verwerken in overeenstemming met deze principes.

Rechtmatige grondslag
Persoonsgegevens worden door de organisaties slechts verwerkt in overeenstemming met de wet en op een behoorlijke en zorgvuldige wijze. Dit betekent onder meer dat verwerkingen alleen plaatsvinden indien hiervoor een rechtmatige verwerkingsgrondslag bestaat. Veelal vloeit de grondslag voor een verwerking bij een gemeente voort uit een wet (wettelijke verplichting) of een publiekrechtelijke taak.

Welbepaalde doeleinden
De organisaties verwerken persoonsgegevens voor zeer uiteenlopende doeleinden. Zonder concreet doel mogen persoonsgegevens niet worden verwerkt. De verwerking van persoonsgegevens vindt plaats op een wijze die noodzakelijk is om de doeleinden te realiseren waarvoor de gegevens zijn verkregen. Dit betekent dat de organisaties alleen die persoonsgegevens verwerken die noodzakelijk zijn voor het gestelde doel (ter zake dienend). De organisaties zien af van de verwerking als het doel op een andere – minder ingrijpende – wijze kan worden bereikt, bijvoorbeeld, door minder of geen persoonsgegevens te verwerken.

Verdere verwerking
Persoonsgegevens kunnen in bepaalde gevallen verder worden verwerkt voor andere doelen dan waarvoor ze in eerste instantie zijn verzameld. Daarbij geldt onder andere dat de verdere verwerking verenigbaar moet zijn met het initiële doel, er zich geen nadelige effecten voor de betrokkenen voordoen, dan wel dat hiervoor extra waarborgen zijn getroffen. De organisaties voeren, voordat de verdere verwerking start, een toets uit om te bepalen of de verdere verwerking verenigbaar is met de initiële doeleinden en er voldoende waarborgen zijn voor de bescherming van de persoonlijke levenssfeer.

Minimale gegevensverwerking
Gegevens mogen alleen worden verwerkt als dit in verhouding staat tot het doel. Als het doel waarvoor persoonsgegevens worden verwerkt, zonder of met minder persoonsgegevens kan worden bereikt, dan kiezen de organisaties bij voorkeur voor die mogelijkheid. Ook als het doel waarvoor persoonsgegevens worden verwerkt op een wijze kan worden verwezenlijkt die minder inbreuk maakt op de privacy van de betrokkene, dan kiezen de organisaties bij voorkeur voor die mogelijkheid.

Juiste en actuele gegevens
De organisaties zorgen ervoor dat alleen persoonsgegevens worden verwerkt die juist en actueel zijn, gelet op het doel waarvoor ze zijn verzameld of verder worden verwerkt. De organisaties nemen passende maatregelen om persoonsgegevens juist en actueel te houden.

Gegevens worden op tijd vernietigd

De organisaties stellen de bewaartermijn van een verwerking vast aan de hand van wettelijke bepalingen en de selectielijsten. Gemeenten hebben op grond van de Archiefwet 1995 onder andere de plicht om zogenaamde selectielijsten op te stellen. Deze selectielijsten bepalen voor een 'selectie van documenten' hoelang deze moeten worden bewaard.

Alleen als de bewaartermijn niet op basis van wettelijke bepalingen of de selectielijsten kan worden vastgesteld, stellen de organisaties de bewaartermijn vast op basis van noodzakelijkheid. Persoonsgegevens mogen niet langer worden bewaard dan noodzakelijk. De organisaties bewaren gegevens alleen langer als deze geanonimiseerd worden, zodat directe of indirecte identificatie van een persoon niet meer mogelijk is, bijvoorbeeld ten behoeve van statistische doeleinden.

Integriteit en vertrouwelijkheid
De organisaties nemen, met name rekening houdend met de verwerkingsrisico's, passende technische en organisatorische maatregelen om de persoonsgegevens te beschermen tegen misbruik en onrechtmatige of ongeautoriseerde verwerking. De organisaties handelen hierbij in overeenstemming met het informatiebeveiligingsbeleid. Het informatiebeveiligingsbeleid verplicht de organisaties informatie te beveiligen tegen ongeautoriseerd gebruik, vernietiging (per ongeluk of onrechtmatig), verlies of vervalsing, onbevoegde bekendmaking of toegang en alle andere onrechtmatige manieren van verwerking.

Gegevensbescherming door ontwerp en door standaardinstellingen (Privacy by Design en Privacy by Default)
De organisaties houden bij de ontwikkeling van nieuwe diensten, systemen of processen rekening met aspecten van gegevensbescherming in het kader van privacywetgeving om zo te komen tot een zo optimaal mogelijke bescherming van persoonsgegevens. Dit uitgangspunt wordt Privacy by Design genoemd. De organisaties dragen er zorg voor dat concrete maatregelen zoveel mogelijk doorgevoerd worden in het ontwerp. Daarbij nemen de organisaties Privacy by Default als uitgangspunt: de standaardinstellingen zijn altijd zo privacy-vriendelijk mogelijk.

Toegang tot gegevens
Uitsluitend geautoriseerde medewerkers zijn bevoegd tot het invoeren, rechtstreeks raadplegen, wijzigen en verwijderen van persoonsgegevens voor zover aan hen hiervoor bevoegdheden zijn toegekend. Deze bevoegdheden worden verleend op grond van het binnen de organisaties geldend beleid voor toegang tot gegevens, waaronder het informatiebeveiligingsbeleid. Het beheer van bevoegdheden wordt periodiek gecontroleerd. De organisaties hanteren daarnaast oplossingen en toepassingen, waaronder het bijhouden van loggegevens om ongeautoriseerde toegang tot en niet toegestane verwerkingen van persoonsgegevens zo veel mogelijk te beperken en passend daarop te reageren.

Inbreuk in verband met persoonsgegevens
Bij toegang tot, verlies of wijziging van persoonsgegevens zonder dat dit de bedoeling is, is er sprake van een datalek. Dat moet, afhankelijk van het risico, worden gemeld bij de toezichthouder (de Autoriteit Persoonsgegevens) en bij de personen op wie de persoonsgegevens betrekking hebben. De organisaties registreren datalekken, formuleren verbeterpunten en zien toe op de opvolging hiervan. Nadere regels ten aanzien van het vaststellen, melden en afhandelen van datalekken zijn opgenomen in een procedure met betrekking tot meldingen van datalekken en informatiebeveiligingsincidenten.

Samenwerking
Verwerkers
De organisaties schakelen soms derden in om persoonsgegevens in opdracht van en ten behoeve van hen te verwerken. Deze derden kunnen in bepaalde gevallen kwalificeren als verwerker. De AVG en Wpg verplichten organisaties tot het maken van contractuele afspraken met verwerkers. De organisaties gebruiken hiervoor verwerkersovereenkomsten in lijn met landelijke afspraken vanuit de Vereniging van Nederlandse Gemeenten (VNG).

Samenwerkingsverbanden
Verder kan het voorkomen dat de organisaties samenwerken met andere (overheids)organisaties. In die gevallen kan sprake zijn van meerdere verwerkersverantwoordelijken (gezamenlijk of individueel). De organisaties maken hierbij duidelijke afspraken over de verwerking van persoonsgegevens. Gewaarborgd wordt dat de taken en verantwoordelijkheden voldoende belegd zijn zodat de rechten en vrijheden van betrokkenen zijn gewaarborgd.

Doorgifte buiten de EER
Doorgifte van persoonsgegevens aan landen buiten de Europese Economische Ruimte (EER) of een internationale organisatie, geschiedt alleen in overeenstemming met de relevante bepalingen in toepasselijke wet- en regelgeving en dit privacybeleid.

Transparantie
De organisaties informeren de betrokkenen tijdig, op een eenvoudige, begrijpelijke en toegankelijke wijze over het feit dat zij persoonsgegevens verwerken, op welke wijze en voor welke doeleinden. De betrokkenen worden op een heldere en laagdrempelige wijze geïnformeerd over hun rechten en hoe zij deze rechten uit kunnen oefenen. Alleen indien de wet anders bepaalt, wijken de organisaties van deze informatieplicht af.

Rechten van betrokkenen
Betrokkenen hebben verschillende rechten vanuit de AVG om meer controle te houden over hun persoonsgegevens. Te weten het recht van inzage, recht op rectificatie, recht op verwijdering, recht op bezwaar, recht op beperking en recht op overdraagbaarheid. Nadere regels ten aanzien van de rechten van betrokkenen zijn opgenomen in de procedure rechten van betrokkenen.

Geschillenbeslechting
Indien betrokkenen van mening zijn dat de organisaties niet op een juiste wijze met hun persoonsgegevens zijn omgegaan, kunnen zij een klacht indienen via de klachtenprocedure zoals opgenomen op de gemeentelijke websites. De betrokkene heeft ook het recht een klacht in te dienen bij de Autoriteit Persoonsgegevens, met betrekking tot de naleving van wet- en regelgeving op het gebied van de bescherming van persoonsgegevens.

Verantwoording en toezicht
Onder de verantwoordelijkheid van zowel de colleges van B&W, het bestuur van de bedrijfsvoeringseenheid als de gemeenteraden vindt een groot aantal verwerkingen van persoonsgegevens plaats. Daar vindt extern en intern toezicht op plaats. De Autoriteit Persoonsgegevens (AP) houdt toezicht op de naleving van de privacyregels in Nederland. Daarnaast beschikken de organisaties over een interne toezichthouder: de Functionaris Gegevensbescherming (FG). De FG ziet erop toe dat de AVG intern wordt nageleefd. De organisaties stellen voldoende middelen ter beschikking aan de FG om het toezicht adequaat uit te kunnen voeren.

Verwerkingsregister
De organisaties beschikken over een actueel verwerkingsregister, waarin alle verwerkingen van persoonsgegevens gedocumenteerd zijn en inzichtelijk zijn gemaakt.

Gegevensbeschermingseffectbeoordeling /Data protection impact assessment (hierna: DPIA)
Om te kunnen bepalen of een verwerking waarschijnlijk een hoog risico inhoudt voeren de organisaties een beknopte risico inventarisatie in het kader van gegevensbescherming ofwel een pré DPIA uit. Als een verwerking waarschijnlijk een hoog risico inhoudt voor de betrokkene, moeten de organisaties een beoordeling uitvoeren van het effect van deze verwerking van persoonsgegevens (DPIA). Als uit de DPIA blijkt dat er inderdaad hoge risico's zijn verbonden aan de verwerking, moeten de organisaties passende maatregelen nemen om de risico's te verminderen. Als het niet lukt passende maatregelen te nemen om de risico's voldoende te verminderen, dan moeten de organisaties met de AP overleggen, voordat zij met de verwerking starten. Dit wordt een voorafgaande raadpleging genoemd.

Functionaris gegevensbescherming (FG)
De organisaties zijn overheidsinstanties die structureel en op grote schaal persoonsgegevens verwerken, waaronder bijzondere persoonsgegevens. De organisaties zijn daarom wettelijk verplicht om een FG aan te stellen. De FG is de onafhankelijke interne toezichthouder en heeft een adviserende, informerende en toezichthoudende taak. Dit betekent dat de FG toeziet op alle verwerkingen van persoonsgegevens. De organisaties voorzien de FG van voldoende middelen om zijn taken uit te kunnen voeren. De FG heeft de bevoegdheid ruimtes te betreden, zaken te onderzoeken en inlichtingen en inzage te vragen. De FG kan vrij en onafhankelijk advies uitbrengen. Hij heeft een autonome rol en ontvangt geen instructies van de verwerkingsverantwoordelijken. De FG krijgt geen andere taken of plichten opgelegd die kunnen leiden tot een belangenconflict. Het advies van de FG is niet bindend maar wel zwaarwegend. Het advies wordt vastgelegd en opgenomen in het relevante dossier van de verwerking.

PDCA Cyclus
De organisaties streven ernaar rondom de verwerking van persoonsgegevens in control te zijn en daarover op professionele wijze verantwoording af te leggen. In control betekent in dit verband dat de organisaties weten welke maatregelen genomen zijn ten aanzien van de verwerking van persoonsgegevens, dat er een plan is ten aanzien van de maatregelen die nog niet genomen zijn en dat dit geheel verankerd is in een Plan-Do-Check-Act-cyclus.

Bewustwording
Beleid en maatregelen zijn niet voldoende om risico's op het terrein van het verwerken van persoonsgegevens uit te sluiten. Het is noodzakelijk om het bewustzijn in de organisaties over de risico's met

betrekking tot gegevensbescherming voldoende te creëren en voortdurend te onderhouden. Hierbij dient zowel aandacht te worden besteed aan kennis als veilig gedrag. Iedere medewerker wordt aantoonbaar geïnformeerd over het zorgvuldig omgaan met persoonsgegevens, bijvoorbeeld via gedragsregels en instructies. Dit gebeurt passend binnen en bij het domein waarbinnen de gegevens worden verwerkt.

7. Rollen, taken, bevoegdheden en Verantwoordelijken

Het governancemodel van de organisaties biedt een overkoepelende visie en strategie hoe de bescherming van persoonsgegevens effectief belegd wordt binnen de organisatie. Daartoe bevat het een beschrijving van de rollen, taken en verantwoordelijkheden van onder andere het College van B&W, het managementteam en medewerkers, de Functionaris voor de Gegevensbescherming (FG) en de CISO.

Gemeenteraad
De raad, als hoogste bestuursorgaan in de gemeente, is verantwoordelijk voor de verwerkingen door de griffie, de raadscommissies en de HRM-verwerkingen met betrekking tot de griffie. Daarnaast heeft de raad een bestuurlijke toezicht taak op basis van de Gemeentewet en de decentralisatiewetgeving. Verder is de raad verantwoordelijk voor het aanstellen van een Functionaris gegevensbescherming voor zover het de eigen bevoegdheden betreft.

College van B&W
De Colleges zijn eindverantwoordelijk voor de naleving van de privacywetgeving binnen de gemeenten. De Colleges en het bestuur van de bedrijfsvoeringseenheid hebben de volgende taken en verantwoordelijkheden:
- Stellen het privacybeleid vast op basis van wet- en regelgeving;
- Stellen de gedragsregels voor medewerkers vast met betrekking tot gegevensbescherming;
- Zijn verantwoordelijk voor het aanstellen van de FG voor zover het de eigen bevoegdheden betreft;
- Geven sturing aan privacy beleidsuitvoering en leggen rekenschap af over privacy beleidsuitvoering aan de FG;
- Evalueren de toepassing en werking van het privacybeleid op basis van de rapportage van de FG;
- Leggen verantwoording af aan de raad waar het gaat om risico's en beheersmaatregelen aangaande gegevensbescherming
- Bevorderen een duurzame privacycultuur.

Directie
De directies zijn ambtelijk verantwoordelijk voor kaderstelling en sturing. De directies zorgen dat verwerkingen primair vallen onder de verantwoordelijkheid van de afdelingshoofden of managers. De directies hebben de volgende taken en verantwoordelijkheden:
- Ambtelijk verantwoordelijk voor de naleving van privacywetgeving en het privacybeleid binnen de eigen organisatie;
- Informeren de FG op welke manier de eigen organisatie compliant is aan de privacywetgeving;
- Bevorderen van een duurzame privacycultuur;
- Stellen kaders, operationele procedures, richtlijnen en het jaarplan vast met betrekking tot gegevensbescherming die afdelingsoverstijgend zijn
- Zorgen dat de FG tijdig en naar behoren betrokken wordt bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens.

Afdelingshoofden en managers
De afdelingshoofden en managers zijn operationeel verantwoordelijk voor de bedrijfsprocessen inclusief de verwerkingen van persoonsgegevens binnen hun eigen afdeling. De afdelingshoofden en managers hebben de volgende taken en verantwoordelijkheden:
- Verantwoordelijk voor de naleving van privacywetgeving, het privacybeleid en de gedragsregels met betrekking tot gegevensbescherming binnen de eigen afdeling;
- Verantwoordelijk voor de implementatie en uitvoering van het privacybeleid binnen de eigen afdeling;
- Informeren de FG op welke manier de eigen afdeling compliant is aan de privacywetgeving;
- Verantwoordelijk voor (laten) volgen van trainingen door werknemers binnen de eigen afdeling;
- Sluiten (verwerkers)overeenkomsten af met (keten)partners en leveranciers in het kader van gegevensbescherming;
- Verantwoordelijk voor het registreren en beheren van de gegevensverwerkingen in het verwerkingenregister voor zover deze betrekking hebben op de eigen afdeling;
- Verantwoordelijk voor het treffen van passende maatregelen in het kader van informatiebeveiliging en gegevensbescherming in het kader van privacy op basis van risicomanagement;

- Verantwoordelijk voor het uitvoeren van risicobeoordelingen op processen in het kader van privacywetgeving (pré DPIA's en indien nodig DPIA's);
- Bevorderen van een duurzame privacycultuur;
- Zorgen dat de FG tijdig en naar behoren betrokken wordt bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens.

Functionaris Gegevensbescherming (FG)
Op basis van de AVG en Wpg is het aanstellen van een FG verplicht voor de organisaties. De FG is verantwoordelijk voor het interne toezicht op de naleving van de AVG en Wpg. De FG heeft een onafhankelijke adviserende en toezichthoudende positie in de organisatie. De FG heeft de volgende taken, verantwoordelijkheden en bevoegdheden zoals ook deels beschreven in artikel 39 van de AVG:
- Houdt toezicht op, adviseert en informeert de verwerkingsverantwoordelijken over hun verplichtingen in het kader van privacywetgeving;
- Monitort veranderingen in wetgeving en stelt de impact van deze wijzigingen vast en adviseert de organisatie bij de implementatie hiervan;
- Ondersteunt de verwerkingsverantwoordelijken bij het opstellen van beleid, voorschriften, procedures en modelovereenkomsten;
- Draagt het privacybeleid actief uit binnen de gehele gemeente en bevordert een cultuur van duurzame gegevensbescherming;
- Treedt op als contactpunt van en werkt samen met de Autoriteit Persoonsgegevens
- Fungeert als contactpersoon voor personen die gebruik willen maken van hun privacyrechten (ombudsfunctie);
- Adviseert verwerkingsverantwoordelijken ten aanzien van het mitigeren van privacy risico's, bijvoorbeeld bij het uitvoeren van pré DPIA's, DPIA's en hoog-risico dossiers;
- Adviseert over de bepalingen in (verwerkers-)overeenkomsten en faciliteert bij het opstellen, aanpassen en uitonderhandelen daarvan;
- Adviseert over mechanismen voor internationale uitwisseling van persoonsgegevens naar landen buiten de EU/EER;
- Adviseert de verwerkingsverantwoordelijke over Privacy by Design & Default bij ontwikkeling van nieuwe systemen in samenwerking met de CISO;
- Adviseert en ondersteunt de verwerkingsverantwoordelijke bij datalekken;
- Stimuleert actief het bewustzijn bij medewerkers voor een integere omgang met persoonsgegevens;
- Plant en bewaakt onderzoeken naar de bescherming van persoonsgegevens, in samenwerking met concern-control en eventuele externe auditors;
- Beschikt over controle- en monitoringbevoegdheden (het recht om interne onderzoeken te laten uitvoeren met toegang tot informatie).

De FG kan worden ondersteund door een Privacy Officer en Privacy&Security Contactpersonen op de afdelingen.

Chief Information Security Officer (CISO)
De Chief Information Security Officer (CISO) ondersteunt vanuit een onafhankelijke positie de organisatie bij het bewaken en verhogen van de betrouwbaarheid van de informatievoorziening. Informatiebeveiliging is een randvoorwaarde voor de bescherming van persoonsgegevens. De CISO heeft de volgende taken en verantwoordelijkheden:
- Verantwoordelijk voor het (doen) implementeren, adviseren en toezicht houden ten aanzien van het informatiebeveiligingsbeleid en Baseline Informatiebeveiliging Overheid (BIO);
- Adviseert de verwerkingsverantwoordelijke over Security by Design & Default bij ontwikkeling van nieuwe systemen in samenwerking met de FG;
- Coördineert en adviseert bij afhandelen van beveiligingsincidenten;
- Contactpersoon voor de Informatiebeveiligingsdienst gemeenten (IBD);
- Formuleert het Informatiebeveiligingsbeleid en uitwerking daarvan in richtlijnen, voorschriften en procedures;
- Adviseert bij en begeleidt risicoanalyses en GAP-analyses BIO;
- Zorgt voor voorbereiding op toekomstige informatiebeveiligingsrisico's en ICT-beveiligingsrisico's mede op basis van het dreigingsbeeld Nederlandse Gemeenten;
- Informeert bestuur en management over de status van informatiebeveiliging en incidenten en presenteert verbetervoorstellen.

De CISO kan worden ondersteund door een Information Security Officer (ISO) en Privacy&Security contactpersonen.

Inwerkingtreding

Dit privacybeleid treedt een dag na bekendmaking in werking. Het Privacybeleid Bommelerwaard wordt per die datum ingetrokken. Het beleid wordt tweejaarlijks geëvalueerd en indien nodig herzien. Aanpas-

singen aan dit beleid worden bekendgemaakt. De meest actuele versie van het beleid is te vinden op de website van de gemeente.

Aldus vastgesteld in de collegevergadering van 11 april 2023,

J.W. Lange
Secretaris

H. van Kooten
Burgemeester