GEMEENTE Reusel-De Mierden

GEMEENTEBLAD

Officiële uitgave van de gemeente Reusel-De Mierden

Nr. 377672

4 september 2024

Privacybeleid 2024 gemeente Reusel-De Mierden

Intitulé

Privacybeleid 2024 gemeente Reusel-De Mierden

Het college van de gemeente Reusel-De Mierden

Gelet op het artikel 24:2 van de Algemene Verordeing Gegevensbescherming

B e s l u i t

Vast te stellen de volgende beleidsregel: Privacybeleid 2024 gemeente Reusel-De Mierden

Privacybeleid 2024 gemeente Reusel-De Mierden

1. Inleiding

Als gemeente zijn wij verplicht te voldoen aan de 'verantwoordingsplicht' zoals bepaald in de Algemene Verordening Gegevensbescherming (AVG). We treffen passende technische en organisatorische maatregelen voor de verwerking van persoonsgegevens in de vorm van een zogenaamd gegevensbeschermingsbeleid, oftewel privacybeleid. Het privacybeleid was voor het laatst vastgesteld in 2018 en wordt nu geactualiseerd. Dit is gebeurd op basis van het in 2022 opgestelde algemene privacybeleid- en reglement van de andere Kempengemeenten, de Samenwerking Kempengemeenten, KempenPlus en onze Functionaris Gegevensbescherming.

In dit privacybeleid staat beschreven hoe wij als gemeente omgaan met de privacy van burgers.

De gemeente Reusel-De Mierden werkt met (persoons)gegevens van burgers, ondernemers, medewerkers en (keten)partners. Deze gegevens worden verzameld om de wettelijke taken goed uit te voeren. Denk hierbij aan taken in het sociaal domein, openbare orde en veiligheidsdomein of op het gebied van dienstverlening. Burgers mogen erop vertrouwen dat onze gemeente zorgvuldig en veilig met deze persoonsgegevens omgaat. Nieuwe wettelijke kaders, technologische ontwikkelingen, innovatieve voorzieningen en een steeds verder gaande digitalisering stellen steeds andere eisen aan de bescherming van deze gegevens en privacy. De gemeente is zich van deze ontwikkelingen bewust en zorgt dat de privacy gewaarborgd blijft. Zij doet dit onder andere door het nemen van maatregelen op het gebied van informatiebeveiliging, dataminimalisatie, transparantie en voorlichting, ondersteuning en training van medewerkers.

Het bestuur en management spelen een cruciale rol bij het waarborgen van de bescherming van persoonsgegevens. Onze gemeente geeft middels dit beleid een duidelijke richting aan privacy en laat zien dat zij het belangrijk vindt privacy van burgers te waarborgen en beschermen. Daarbij is een inte-grale aanpak, goed eigenaarschap en risicobewustzijn van iedereen die persoonsgegevens verwerkt onder verantwoordelijkheid van de gemeente Reusel-De Mierden essentieel.

2. Verwerking van persoonsgegevens

Een verwerking van persoonsgegevens (artikel 4 AVG) is elke handeling of elk geheel van handelin-gen met persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde processen.
In de AVG valt onder een verwerking:
1. verzamelen, vastleggen en ordenen;
2. bewaren, bijwerken en wijzigen;
3. opvragen, raadplegen, gebruiken;
4. verstrekken door middel van doorzending;
5. verspreiding of enige andere vorm van ter beschikkingstellen;
6. samenbrengen, met elkaar in verband brengen;
7. afschermen, uitwissen of vernietigen van gegevens.

Uit deze opsomming blijkt dat alles wat je met een persoonsgegeven doet een verwerking is. Verwerken is daarom een ruim begrip.

De bescherming van persoonsgegevens speelt een belangrijke rol in de relatie tussen de burgers en de overheid. De gemeente, haar bestuurders en medewerkers hebben de verantwoordelijkheid over de verwerking van persoonsgegevens bij alle taken:
- die zij zelf uitvoert;.
- die voor haar worden uitgevoerd op basis van mandaat en;
- waar zij bij de uitvoering betrokken is.

Voor wat betreft de laatstgenoemde taken worden bijvoorbeeld de samenwerkingsverbanden binnen het sociaal- en veiligheidsdomein bedoeld.

In elk gemeentelijk werkproces vinden verwerkingen van persoonsgegevens plaats. Met andere woorden: bij alles wat wij doen moeten wij rekening houden met de bescherming van persoonsgegevens. De bescherming van persoonsgegevens omvat de verplichting om zorgvuldig, veilig, proportioneel en vertrouwelijk om te gaan met het verzamelen, bewaren en beheren van deze persoonsgegevens. Proportioneel betekent dat je alleen die persoonsgegevens mag gebruiken die je voor de taak nodig hebt en zo lang als je ze hiervoor nodig hebt. Al het andere is niet toegestaan.

Elke medewerker moet zijn of haar verantwoordelijkheden kennen bij het verwerken van persoonsgegevens en erop attent zijn conform de vereisten van de AVG te werken. Hierdoor worden de risico's, zoals de kans op een datalek kleiner. Medewerkers moeten de vaardigheden bezitten om goed en zorgvuldig met persoonsgegevens om te gaan en hierbij in hun werk voldoende ondersteund worden. Technisch is het beschermen van de persoonsgegevens complex en het wordt steeds complexer. Dit komt door de snelle technologische ontwikkelingen. Voor onze gemeentelijke ICT systemen, het Kempennetwerk plus zijn verbindingen en de hardware wordt de technische ondersteuning uitgevoerd door Shared Service Centrum de Kempen (SSC).
Functioneel beheer van applicaties, gegevens en informatie voert de gemeente zelf uit. Ook hier hebben we te maken met groeiende complexiteit, veroorzaakt door de toenemende samenhang van taken (als gevolg van decentralisatie), grote uitdagingen op het terrein van veiligheid (spyware, hacken, etc.) en elkaar snel opvolgende nieuwe wet- en regelgeving.

3. Reikwijdte

Dit privacybeleid is van toepassing op:
1. Alle persoonsgegevens die gemeente Reusel-De Mierden verwerkt of laat verwerken, zowel fysiek als digitaal, zowel intern als extern;
2. Alle taken en processen waarin persoonsgegevens worden verwerkt waar gemeente Reusel-De Mierden verantwoordelijk voor is;
3. Alle personen en/of organisaties die persoonsgegevens van de gemeente Reusel-De Mierden verwerken onder verantwoordelijkheid van ons college;

4. Alle organisatorische, procedurele en technische maatregelen ter bescherming van persoonsgegevens.

3.1 Sociaal domein

Voor het sociaal domein is specifiek beleid opgesteld voor de uitwisseling van persoonsgegevens voor de taken die gedelegeerd zijn aan de Samenwerking Kempengemeenten en KempenPlus. In de volgende stukken is vastgelegd hoe er binnen de gedelegeerde taken van het sociaal domein wordt omgegaan met privacygevoelige informatie:

Privacybeleid GRSK	Versie 2022-2025 en toekomstige versies
Privacybeleid KempenPlus	Versie 2022-2025 en toekomstige versies
Privacybeleid Sociaal Domein Kempengemeenten	Versie 2018 en toekomstige versies

De gemeente Reusel-De Mierden voert sommige (deel)processen binnen het sociaal domein zelf uit, zoals de taken van het loket A tot Z. Ook voor deze taken geldt dit privacybeleid. Uitgangspunt is dat dit gemeentelijke privacybeleid de gegevensdeling in het sociaal domein niet hindert zolang dit binnen de wettelijke kaders gebeurt.

4. Wettelijke kaders

Het privacybeleid van de gemeente Reusel-De Mierden is in lijn met het algemene beleid van de gemeente en de relevante lokale, regionale, nationale en Europese wet- en regelgeving. De gemeente is zelf verantwoordelijk voor het opstellen, uitvoeren en handhaven van het beleid. Hiervoor gelden meerdere wettelijke kaders. De Algemene Verordening Gegevensbescherming (AVG) en de Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG) bevatten de algemene regels voor de omgang met persoonsgegevens. Daarnaast is er wet- en regelgeving die op een specifiek taakveld van toepassing is. Deze staan beschreven in bijlage 1.
In dit beleid worden de begrippen overeenkomstig de AVG gehanteerd. De term ‘privacy’ wordt gebruikt in de betekenis van 'gegevensbescherming’. Overige veel gebruikte begrippen zijn te raadplegen in bijlage 2.

5. Basisprincipes (beginselen) AVG

De AVG kent 6 basisprincipes, in de AVG 'beginselen' genoemd. De 6 AVG-beginselen zijn:
1. rechtmatigheid, behoorlijkheid en transparantie;
2. doelbinding;
3. dataminimalisatie;
4. juistheid;
5. opslagbeperking;
6. vertrouwelijkheid en integriteit.

Iedereen die persoonsgegevens verwerkt, moet zich hieraan houden en dit kunnen aantonen. Dat is het zevende, overkoepelende beginsel van de AVG: de verantwoordingsplicht.

5.1 Rechtmatigheid, behoorlijkheid, transparantie

De wet zegt 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:
1. om een verplichting na te komen die in de wet staat;
2. voor de uitvoering van een overeenkomst waar de betrokkene onderdeel is;
3. om de vitale belangen van de betrokkene te beschermen;
4. voor de goede vervulling van de gemeentelijke taak (van algemeen belang of voor de uitoe-fening van openbaar gezag);
5. wanneer de betrokkene toestemming heeft gegeven voor de specifieke verwerking.

Persoonsgegevens worden in overeenstemming met de wet- en regelgeving en op behoorlijke en zorgvuldige wijze verwerkt. Zorgvuldige en behoorlijke verwerking houdt in ieder geval een transparantieplicht in. Burgers en andere personen die op de een of andere manier te maken hebben met de gemeente moeten weten dat en waarom hun gegevens worden verwerkt. Als zij om inzage in de verwerking van hun persoonsgegevens vragen, gaat de gemeente dit faciliteren.

De gemeente informeert de betrokkenen tijdig, op een zo begrijpelijke en toegankelijke wijze over het feit dat zij persoonsgegevens verwerkt, op welke wijze en voor welke doeleinden. De betrokkene wordt op heldere en laagdrempelige wijze geïnformeerd over zijn rechten en de wijze waarop hij deze kan uitoefenen via het privacystatement op de website. Burgers kunnen een AVG-verzoek bij de ge-meente indienen.

5.2 Grondslag en doelbinding
Persoonsgegevens mogen alleen verzameld worden met een gerechtvaardigd doel (artikel 5 AVG). Dat doel moet specifiek zijn en vooraf uitdrukkelijk zijn omschreven. Persoonsgegevens mogen dus alleen verwerkt worden als ze op dat moment nodig zijn voor de uitvoering van een taak en mogen niet voor andere doelen verwerkt worden. Voor de uitvoering van sommige wetten zijn de doelen voor het ver-werken in de wet al vastgelegd, net als de persoonsgegevens die verwerkt mogen worden.
Verwerkingen met de daar bijbehorende grondslag zijn terug te vinden in het gemeentelijke verwer-kingsregister.

5.3 Dataminimalisatie
De gemeente verwerkt alleen de persoonsgegevens die minimaal noodzakelijk zijn voor het vooraf bepaalde doel. Waar mogelijk worden minder of geen persoonsgegevens verwerkt.
De gemeente houdt bij de start van het ontwerpen of inrichten van informatiesystemen rekening met privacy en beveiliging van persoonsgegevens. Dit wordt ook wel Privacy by Design genoemd. De in-richting van informatiesystemen, website en dergelijke wordt dusdanig georganiseerd dat maximale privacy en beveiliging van persoonsgegevens wordt geborgd (Privacy by default). Medewerkers krij-gen alleen autorisaties voor applicaties die voor hun werk noodzakelijk zijn.

5.4 Subsidiariteit en proportionaliteit
Voor het bereiken van het doel waarvoor de persoonsgegevens worden verwerkt, wordt inbreuk op de persoonlijke levenssfeer van de betrokken burger zoveel mogelijk beperkt. De inbreuk op de belan-gen van de betrokkene mag niet onevenredig zijn in verhouding tot het met de verwerking te dienen doel.

5.5 Integriteit en vertrouwelijkheid
De gemeente gaat zorgvuldig om met persoonsgegevens en behandelt deze vertrouwelijk. Zo worden persoonsgegevens alleen verwerkt door bevoegde personen met een geheimhoudingsplicht en voor het doel waarvoor deze gegevens zijn verzameld. Indien het doel is behaald, zullen gegevens niet langer worden bewaard dan wettelijk vereist is. Daarnaast zorgt de gemeente voor passende beveili-ging van persoonsgegevens. Deze beveiliging is vastgelegd in het 'Informatiebeveiligingsbeleid Kempengemeen-ten, GRSK en Kempenplus'.

6. Verantwoordelijkheden

Elke medewerker is zelf verantwoordelijk voor de bescherming van de privacy van persoonsgegevens van betrokkenen in zijn of haar werk. Het college van burgemeester en wethouders is eindverantwoor-delijk voor de waarborging van de privacy binnen de ambtelijke organisatie.
Raadsleden en medewerkers van de griffie zijn verantwoordelijk voor de bescherming van de privacy van persoonsgegevens van betrokkenen. De gemeenteraad is eindverantwoordelijk voor de bescher-ming van persoonsgegevens door de griffie.

De Privacy Officer (PO) is binnen de gemeente verantwoordelijk voor het ontwikkelen en bewaken van het privacybeleid. Tevens biedt de PO ondersteuning aan medewerkers bij de uitvoering van het pri-vacybeleid in het dagelijkse werk.

Daarnaast heeft de gemeente een onafhankelijke Functionaris Gegevensbescherming (FG) aangesteld (Artikel 37 t/m 39 AVG). Deze functionaris werkt voor alle Kempengemeenten en is in dienst van de GRSK. De taken van de FG zijn: informeren, adviseren, toezichthouden, bewustwording creëren en optreden als contactpersoon van de Autoriteit Persoonsgegevens (AP). Daarnaast is de FG verant-woordelijk voor het structureel toetsen van de implementatie en de uitvoering van de wettelijke eisen en de gemeentelijke richtlijnen op het gebied van privacy en stelt deze een jaarverslag op met o.a. be-vindingen en aanbevelingen met betrekking tot gegevensbescherming binnen onze gemeente.
Het is niet de bedoeling dat de FG de taken op het gebied van bescherming van de privacy van de PO of de medewerkers zelf overneemt. Eenieder heeft hierin een eigen verantwoordelijkheid.

Onderstaande tabel brengt de verantwoordelijkheden in beeld:

Eindverantwoordelijk	Gemeenteraad

	College van Burgemeester en Wethouders Burgemeester
Feitelijk verantwoordelijk	Griffier Managementteam
Uitvoerend	Alle medewerkers (inclusief inhuur/extern)
Adviserend / ondersteunend	Functionaris Gegevensbescherming (FG) Privacy Officer (PO) Chief Information & Security Officer (CISO)
Controlerend	Concerncontroller / Controller informatiebevei-liging Functionaris Gegevensbescherming
Toezichthoudend	Functionaris Gegevensbescherming Autoriteit Persoonsgegevens (AP)

7. Transparantie

7.1 Wet open overheid (Woo)
De Wet open overheid (Woo) biedt eenieder de mogelijkheid om publieke informatie op te vragen bij de gemeente. Bij het verzoek bekijkt de gemeente altijd of het antwoord geen inbreuk maakt op de persoonlijke levenssfeer van betrokkenen. In principe worden er geen persoonsgegevens verstrekt. Bij het voldoen aan een Woo-verzoek wordt de te verstrekken informatie eerst geanonimiseerd.

7.2 Wet hergebruik van overheidsinformatie
De Wet hergebruik van overheidsinformatie regelt het op verzoek verstrekken van overheidsinformatie voor hergebruik. Bij het verzoek bekijkt de gemeente ook altijd of het verstrekken van gegevens geen inbreuk maakt op de persoonlijke levenssfeer van betrokkenen. In principe worden er geen persoonsgegevens verstrekt. Onze openbare dataset van gegevens zoals bedoeld in de Wet hergebruik van overheidsgegevens bevat geen gegevens die herleidbaar zijn naar een persoon.

7.3 Informatieplicht (Artikel 13,14 AVG)
De gemeente informeert betrokkenen over het verwerken van persoonsgegevens. Wanneer betrokkenen gegevens aan de gemeente verstrekken, worden zij op de hoogte gesteld van de manier waarop de gemeente met persoonsgegevens om zal gaan. Als er geen toestemming is gegeven door de betrokkene worden gegevens niet openbaar gemaakt tenzij dit wettelijk vereist is. De betrokkene wordt niet nogmaals geïnformeerd als hij/zij al weet dat de gemeente 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 (buiten de betrokkene om), wordt de betrokkene geïnformeerd op het moment dat deze persoonsgegevens voor de eerste keer worden verwerkt.

7.4 Verwijdering
De gemeente bewaart de persoonsgegevens niet langer dan nodig is voor de uitvoering van gemeentelijke taken, of zoals vastgelegd in de Archiefwet. Wanneer er nog persoonsgegevens opgeslagen zijn die niet langer nodig zijn om het doel te bereiken, 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. Dit kan bijvoorbeeld door het anonimiseren en/of pseudonimiseren van persoonsgegevens.

7.5 Rechten van betrokkenen (Artikel 13 t/m 20 AVG)
De wet bepaalt niet alleen de plichten van degenen die de persoonsgegevens verwerken, maar be-paalt 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:

1. recht op informatie: betrokkenen hebben het recht om aan de gemeente te vragen of zijn/haar persoonsgegevens worden verwerkt;
2. inzagerecht: betrokkenen hebben de mogelijkheid om te controleren of, en op welke manier, zijn/haar gegevens worden verwerkt door in te zien welke persoonsgegevens er worden ver-werkt;
3. correctierecht: als duidelijk wordt dat de gegevens niet kloppen, kan de betrokkene een ver-zoek indienen bij de gemeente om dit te corrigeren;
4. recht op beperking: betrokkenen hebben het recht aan de gemeente te vragen om minder persoonsgegevens te verwerken;
5. recht om vergeten te worden: in gevallen waar de betrokkene toestemming of geen toestem-ming heeft gegeven om gegevens te verwerken, wanneer de gegevens niet meer nodig zijn of als er bezwaar gemaakt is tegen de verwerking en deze akkoord is bevonden, heeft de betrok-kene het recht om de persoonsgegevens te laten verwijderen;

6. recht op bezwaar: betrokkenen hebben het recht om bezwaar te maken tegen de verwerking van zijn/haar persoonsgegevens.
7. recht op dataportabiliteit: betrokkene heeft het recht om de persoonsgegevens over te dragen naar een andere partij. Niet alle soorten gegevens kunnen overgedragen worden.
8. recht om toestemming in te trekken: zodra een betrokkene toestemming heeft gegeven om zijn persoonsgegevens te mogen verwerken, krijgt hij tegelijkertijd het recht om deze toestemming in te trekken. Het intrekken van de toestemming moet net zo eenvoudig zijn als het geven daarvan.
9. recht niet te worden onderworpen aan een besluit welke gebaseerd is op een uitsluitend geautomatiseerde verwerking.

7.6 Indienen van verzoek
Om gebruik te maken van bovengenoemde rechten kan de betrokkene een verzoek indienen. Dit verzoek kan via de gemeentelijke website worden ingediend, waarbij de betrokkene via DigiD inlogt. Ook kan de betrokkene een afspraak maken om naar het gemeentehuis te komen, waarbij de betrokkene zich met een geldig identiteitsbewijs moet identificeren. Aan de hand van een verzoek kan de gemeente aanvullende informatie opvragen om zeker te zijn van de identiteit van de betrokkene.
De gemeente heeft, vanaf de ontvangst van het verzoek, één maand de tijd om te beoordelen of het verzoek gerechtvaardigd is. Binnen één maand informeert de gemeente betrokkene wat er met het verzoek gaat gebeuren. Wanneer dit niet mogelijk is, kan de reactietermijn met twee maanden worden verlengd. Dit moet dan wel vóór het aflopen van de eerste maand aan de betrokkene gemeld zijn. Als het verzoek niet (volledig) wordt opgevolgd, is er de mogelijkheid voor betrokkene om bezwaar te maken bij de gemeente. Wanneer een verzoek wordt geweigerd kan betrokkene, na eerst contact te hebben opgenomen met de PO of FG, een klacht indienen bij de AP.

8. Verwerkingsregister en verwerkersovereenkomst

Een overzicht van de categorieën van persoonsgegevens welke de gemeente verwerkt, is te vinden in het gepubliceerde verwerkingsregister op de gemeentelijke website. Dit verwerkingsregister wordt periodiek geactualiseerd.

8.1 Register van verwerkingen (Artikel 30 AVG)
De gemeente is verantwoordelijk voor het aanleggen van een register van alle verwerkingen waarvan de gemeente de verwerkingsverantwoordelijke is. Elk register bevat een beschrijving van het proces waarvoor de verwerking plaatsvindt, en welke gegevens daarvoor worden gebruikt, namelijk:
- de naam en contactgegevens van de verwerkingsverantwoordelijke en, mogelijk, de gezamenlijke verwerkingsverantwoordelijke;
- de doelen van de verwerking;
- een beschrijving van het soort persoonsgegevens en de daarbij horende betrokkenen;
- een beschrijving van de ontvangers van de persoonsgegevens;
- een beschrijving van het delen van persoonsgegevens aan een ander land buiten de EER of internationale organisatie;
- de termijnen waarin de verschillende persoonsgegevens moeten worden gewist;
- een algemene beschrijving van de beveiligingsmaatregelen.

8.2 Verwerkersovereenkomsten met derden (Artikel 24 t/m 34 AVG)
De gemeente maakt gebruik van derde partijen in de uitvoering van werkzaamheden waartoe zij zelf geen mogelijkheden bezit. Hierbij valt te denken aan leveranciers van software, netwerkdiensten en dataopslag. De gemeente maakt alleen gebruik van derde partijen als verwerkers van persoonsgegevens (aantoonbaar) voldoende garanties kunnen bieden om de verwerking van (persoons)gegevens te laten voldoen aan de AVG-vereisten. Hiervoor wordt gebruik gemaakt van de modelovereenkomst van de Vereniging Nederlandse Gemeenten (VNG).

9. Geautomatiseerde verwerkingen

9.1 Profilering (Artikel 22 AVG)
Profilering kan plaatsvinden wanneer er een geautomatiseerde verwerking van persoonsgegevens is. Hierbij wordt aan de hand van persoonsgegevens naar bepaalde persoonlijke aspecten van een persoon gekeken met als doel deze persoon te categoriseren en te analyseren, of om zaken te voorspellen. De gemeente Reusel-De Mierden maakt geen gebruik van profilering.

9.2 Algoritmes
De gemeente maakt gebruik van algoritmes en publiceert deze in het Algoritmeregister van de Nederlandse overheid. Algoritmes worden in verschillende programma's gebruikt, bijvoorbeeld in anonimiseringssoftware. Een algoritme herkent hierbij (persoons)gegevens en anderszins vertrouwelijke informatie in een document en doet een voorstel om dit te anonimiseren. Een medewerker beoordeelt het voorstel en voert de aanpassing definitief door. Daarna kan het document, bijvoorbeeld op basis van de Wet open overheid, gepubliceerd worden. Ook Readspeaker, een applicatie op de gemeentelijke website waarmee tekst naar spraak wordt omgezet, maakt gebruik van een algoritme.

9.3 Gebruik van elektronische chips
De gemeente kan voor specifieke doeleinden elektronische chips gebruiken voor het identificeren van een object en het gebruik ervan. Binnen onze gemeente worden er bijvoorbeeld chips gebuikt die gegevens verzamelen voor de afvalverwerking/ het berekenen van de afvalstoffenheffing. De gege-vens in deze chips worden uitgelezen door het inzamelingsbedrijf.
Bij de inzet van chips dient het college van Reusel-De Mierden hiervoor goedkeuring te geven. Middels chips worden daarnaast alleen de gegevens verwerkt die strikt noodzakelijk zijn voor het doel waarvoor ze gebruikt worden.

10. Risico's

Op basis van de AVG is bij schending van privacy het college van burgemeester en wethouders wettelijk verantwoordelijk. De risico's van het verwijtbaar onjuist inzetten of onvoldoende beschermen van persoonsgegevens voor het college kan leiden tot forse boetes, maar ook tot politieke/bestuurlijke schade en imagoschade. De Autoriteit Persoonsgegevens (AP), de landelijke toezichthouder, kan dwangmaatregelen en bestuurlijke boetes opleggen.

10.1 Meldplicht datalekken (Artikel 33,34 AVG)
Er is sprake van een datalek wanneer er een inbreuk ontstaat op de integriteit, vertrouwelijkheid en beschikbaarheid van persoonsgegevens. Hiermee wordt bedoeld als persoonsgegevens onbedoeld in handen vallen van personen die geen toegang tot die gegevens mogen hebben, vernietigd worden of onbetrouwbaar raken. Wanneer er een datalek heeft plaatsgevonden, maakt de privacy officer een registratie van het incident. Indien het datalek mogelijk gevolgen heeft voor de betrokkene, meldt de gemeente dit zo snel mogelijk, maar uiterlijk binnen 72 uur nadat er kennis van de inbreuk is verno-men, aan de AP. Het kan zijn dat de inbreuk een hoog risico met zich meebrengt voor de rechten en vrijheden van de betrokkenen. In dat geval meldt de gemeente dit aan de betrokkenen in duidelijke taal.
Om toekomstige datalekken te voorkomen, worden bestaande datalekken geëvalueerd.
Voor het juist en tijdig beoordelen en afwikkelen van datalekken heeft de gemeente een Procedure meldplicht datalekken vastgesteld.

10.2 Data Protection Impact Assessment (DPIA) (Artikel 35 AVG)
Een Data Protection Impact Assessment (DPIA) is een onderzoek waarbij de effecten en risico's van nieuwe of bestaande verwerkingen worden beoordeeld op de bescherming van de privacy. De gemeente voert deze uit wanneer er een geautomatiseerde verwerking, een grootschalige verwerking, een grootschalige monitoring van openbare ruimten plaatsvindt of wanneer een verwerking een hoog risico inhoudt voor betrokkenen. Dit geldt in het bijzonder voor verwerkingen waarbij nieuwe technologieën worden gebruikt of wanneer verschillende persoonsgegevens met elkaar worden gecombineerd. Deze verwerkingen staan onder andere in (maar zijn niet gelimiteerd tot) de lijst die de AP heeft opgesteld en de criteria van de Europese privacytoezichthouders. Op basis van een opgestelde DPIA wordt afgesproken welke maatregelen er worden genomen om de risico's van de verwerking te beper-ken.

11. Inzet van camera's

11.1 Cameratoezicht
Voor het vergroten van de veiligheid en het beveiligen van (gemeentelijke) eigendommen kan cameratoezicht worden ingezet. De gemeente heeft een zogenoemd 'gerechtvaardigd belang' om deze veiligheid te kunnen waarborgen. Als er iets is gebeurd, kunnen de mensen die daarbij betrokken waren, geïdentificeerd worden via de camerabeelden. Dat zijn dan strafrechtelijke gegevens. Dat die beelden gebruikt mogen worden, staat in art. 33 lid 2 sub b UAVG. 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. Gemeente Reusel-De Mierden heeft dit vastgelegd in een protocol.
Daarnaast kan de burgemeester, onder bepaalde voorwaarden, besluiten tot het inzetten van een tijdelijke camera in de openbare ruimte ten behoeve van de openbare orde en veiligheid. De inzet van het middel (noodzaak) moet in verhouding staan tot de inbreuk op de privacy.

11.2 Bodycams
Voor het gebruik van de bodycams van buitengewoon opsporingsambtenaren (boa's) binnen onze gemeente is een apart protocol opgesteld door de GRSK. Deze bodycams worden namelijk gebruikt in het kader van 'goed werkgeverschap' voor de beveiliging van personen (medewerkers).

12. Slotbepalingen

1. Dit beleid wordt aangehaald als 'Privacybeleid gemeente Reusel-De Mierden'.
2. Dit beleid treedt in werking op de dag na bekendmaking in het Gemeenteblad.
3. Het huidige 'Privacybeleid gemeente Reusel-De Mierden', zoals bekend gemaakt in het Gemeenteblad 2018, 108928, en het huidige 'Privacyreglement gemeente Reusel-De Mierden', zoals bekend gemaakt in het Gemeenteblad 2018, 108925, worden per gelijke datum ingetrokken.

Aldus besloten in de collegevergadering van 20 augustus 2024.
Burgemeester en wethouders van Reusel-De Mierden,
Dhr. J.P.P.S Ruyters
Secretaris
Mw. A.J.M.H. van de Ven
Burgemeester

Bijlage 1: Wettelijke kaders privacybeleid

Voor het opstellen, uitvoeren en handhaven van het privacybeleid gelden onder andere de volgende wettelijke kaders:

1. Europese Algemene Verordening Gegevensbescherming (AVG)
2. Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG)
3. Grondwet (artikel 10 t/m 13)
4. Handvest van de grondrechten van de Europese Unie (EHRM)
5. Europees Verdrag voor de Rechten van de Mens (EVRM) (artikel 8)
6. Wet politiegegevens (Wpg) en het Besluit politiegegevens
7. Wet justitiële en strafvorderlijke gegevens
8. Wet bevordering integriteitsbeoordelingen door het openbaar bestuur (Bibob)

Wetten gericht op de uitvoering in specifieke sectoren zoals:

9. Wet maatschappelijke ondersteuning (WMO)
10. Jeugdwet (voor zover niet gedelegeerd naar de GRSK)
11. Participatiewet (voor zover niet gedelegeerd naar de GRSK)
12. Wet Basisregistratie Personen (BRP)
13. Omgevingswet
14. Wet open overheid (Woo)
15. Archiefwet
16. Drank- en Horecawet
17. Het Wetboek van Strafrecht

Bijlage 2: Definities

AP
De Autoriteit Persoonsgegevens, op grond van de AVG bevoegd om toe te zien op de verwerking van persoonsgegevens overeenkomstig het bij en krachtens de Wet bepaalde.

AVG
Algemene Verordening Gegevensbescherming, VERORDENING (EU) 2016/679 VAN HET EUROPEES PARLEMENT EN DE RAAD, betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens.

Bescherming van persoonsgegevens
Zoals beschreven in artikel 4 van de AVG heeft 'bescherming van persoonsgegevens' niet alleen ten doel ieders privacy te beschermen. Maar ook de integriteit, kwaliteit en veiligheid van de (verwerking van) persoonsgegevens. Dus zorgen dat de juiste, actuele, leesbare persoonsgegevens gebruikt worden en dat die alleen ingezien kan worden door personen die deze gegevens nodig hebben voor hun werk.

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

Dataminimalisatie
Alleen de informatie die noodzakelijk is voor de uitvoering van taken waarvoor een wettelijke grondslag bestaat of toestemming is gegeven.

Data Protection Impact Assessment (DPIA)
Met een DPIA worden de effecten en risico's van nieuwe of bestaande verwerkingen beoordeeld op de bescherming van de privacy.

Functionaris Gegevensbescherming (FG)
Het college van burgemeester en wethouders benoemt een functionaris voor de gegevensbescherming, zoals bedoeld in de AVG, die belast is met toezicht op het privacy- en beveiligingsbeleid van de gemeente.

GRSK
Gemeenschappelijke Regeling Samenwerking Kempengemeenten

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 een e-mailadres dat opgebouwd is uit voorletter en achternaam is ook een persoonsgegeven. Of een gegeven dat iets duidelijk maakt over jouw als persoon. Het voorbeeld hiervan is de pasfoto waaruit je huidskleur blijkt.
Naast gewone persoonsgegevens kent de wet ook bijzondere persoonsgegevens. Dit zijn:

- ras of etnische afkomst;
- politieke opvattingen;
- godsdienst of levensovertuiging;
- lidmaatschap van een vakbond;
- genetische of biometrische gegevens met oog op unieke identificatie;
- gezondheid;
- seksuele leven;

De verwerking van bijzondere persoonsgegeven is verboden tenzij…

Privacy Officer (PO)
De PO is verantwoordelijk voor het ontwikkelen en bewaken van het privacybeleid. Tevens biedt de PO ondersteuning aan bij de uitvoering van dit beleid en is het dagelijkse aanspreekpunt voor mede-werkers voor wat betreft gegevensbescherming.

Profilering
Automatische besluitvorming op basis van het profiel van een inwoner. Een organisatie kan iemands profiel gebruiken om in te schatten hoe diegene zich gaat gedragen. Bijvoorbeeld of deze persoon de rekeningen gaat betalen.

Pseudonimiseren

Een procedure waarmee identificerende gegevens met behulp van een bepaald algoritme in een dataset worden vervangen door versleutelde gegevens (het pseudoniem).

Strafrechtelijke (persoons)gegevens
Strafrechtelijke persoonsgegevens zijn persoonsgegevens die te maken hebben met strafrechtelijke veroordelingen en strafbare feiten. Of met veiligheidsmaatregelen die daarmee verband houden. Onder de AVG gelden speciale regels voor het verwerken van strafrechtelijke gegevens.

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

Verwerking
Een verwerking is alles wat je met een persoonsgegeven doet, zoals: vastleggen, bewaren, verzamelen, bij elkaar voegen, verstrekken aan een ander, en vernietigen.

Verwerkingsverantwoordelijke
De verantwoordelijke voor de verwerking van persoonsgegevens, zoals bedoeld in de AVG, is het college van burgemeester en wethouders, respectievelijk de burgemeester.