gemeente **Roermond**

PRIVACY BELEIDSKADER GEMEENTE ROERMOND 2018-2020

Datum: maart 2018

Versie: 1.2

Inhoudsopgave Privacy beleidskader

1. Kernpunten

1.1. Inleiding

Binnen de gemeente Roermond wordt veel gewerkt met persoonsgegevens[1] van burgers, medewerkers en (keten)partners. Persoonsgegevens worden voornamelijk verwerkt[2] voor het goed uitvoeren van gemeentelijke wettelijke taken. Alle betrokkenen moeten er op kunnen vertrouwen dat de gemeente zorgvuldig en veilig met deze persoonsgegevens omgaat.

In deze tijd gaan ook de gemeenten mee met nieuwe ontwikkelingen. Nieuwe technologische ontwikkelingen, innovatieve voorzieningen, globalisering en een steeds meer digitale overheid stellen andere eisen aan de bescherming van gegevens en privacy. De gemeente Roermond is zich hiervan bewust en zorgt dat privacy gewaarborgd blijft, onder andere door maatregelen op het gebied van informatiebeveiliging, dataminimalisatie, transparantie en gebruikerscontrole.

De gemeente Roermond geeft middels dit privacybeleidskader een duidelijke richting aan en laat zien dat zij de privacy waarborgt, beschermt en handhaaft. Dit privacybeleid is in lijn met de relevante lokale, regionale, nationale en Europese wet- en regelgeving.

1.2. Voor wie?

Het privacybeleidskader gemeente Roermond bevat afspraken tussen het college van burgemeester en wethouders (hierna: “het college”) en het management en vormt daarnaast een kader waarbinnen medewerkers die persoonsgegevens verwerken[2] dienen te opereren.

1.3. Doel

Het doel van dit privacybeleidskader is om kaders vast te leggen waarmee gewaarborgd wordt dat de gemeente Roermond op een behoorlijke en zorgvuldige wijze persoonsgegevens verwerkt in overeenstemming met de wet.

1.4. Visie

Privacy speelt een belangrijke rol in de relatie tussen de burger en de overheid en staat daarmee hoog op de bestuurlijke agenda. Gemeenten dragen verantwoordelijkheid voor persoonsgegevens en gegevensuitwisseling op alle terreinen waar ze actief zijn. Gemeenten zijn verplicht om zorgvuldig en veilig, proportioneel en vertrouwelijk om te gaan met het verzamelen, bewaren en beheren van persoonsgegevens van betrokkenen.

---

[1] Zie artikel 4 sub 1 Algemene Verordening Gegevensbescherming (hierna: “AVG”): persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (“de betrokkene”); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.

[2] Zie artikel 4 sub 2 AVG: verwerking: een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.

Het beschermen van privacy is complex, en wordt steeds complexer door technologische ontwikkelingen (zoals big data en profilering), de decentralisaties, grote uitdagingen op het terrein van veiligheid en nieuwe Europese wetgeving. Deze nieuwe mogelijkheden en ontwikkelingen vragen om een duidelijk (moreel) kompas voor de omgang met persoonsgegevens.

Privacy vormt de basis van onze democratische rechtsstaat. Het is een grondrecht en vormt een vereiste voor het kunnen uitoefenen van andere vrijheden, zoals de vrijheid van meningsuiting en vrije pers. De gemeente Roermond wil het belang van privacy uitdragen en een betrouwbare overheid zijn door in haar handelen de persoonlijke levenssfeer van betrokkenen te eerbiedigen en transparant te zijn over de manier waarop zij dit doet.

1.5. Scope

Dit privacy beleidskader is van toepassing op:

- de gehele organisatie;
- alle processen waarbinnen persoonsgegevens worden verwerkt, waaronder processen die de gemeente Roermond uitbesteedt, inkoopt op een andere manier organiseert voor zover de gemeente voor wat betreft de verwerking van persoonsgegevens als verwerkingsverantwoordelijke[3] (hierna kortheidshalve: “verantwoordelijke”) kan worden aangemerkt;
- informatiesystemen waarin persoonsgegevens worden verwerkt, waarvoor de gemeente (intern en extern) verantwoordelijk is;
- alle ruimten en devices die door gemeente ambtenaren intern en extern worden gebruikt bij de uitoefening van hun taak waar(op) persoonsgegevens worden verwerkt;
- alle onderdelen, objecten en gegevensverzamelingen van de gemeente.

1.6. Raakvlakken en overlap met andere beleidsthema’s

Het privacybeleidskader heeft raakvlakken met andere beleidsthema’s of vertoont hiermee overlap. In dit verband worden met name genoemd:

Informatiebeveiliging
Privacy en informatiebeveiliging staan naast elkaar en zijn van elkaar afhankelijk. Informatiebeveiliging is een randvoorwaarde voor eerbiediging van de persoonlijke levenssfeer bij de verwerking van persoonsgegevens. In het strategisch informatiebeveiligingsbeleid van de gemeente Roermond (laatstelijk vastgesteld 4 november 2016) zijn uitgangspunten beschreven om de beschikbaarheid en integriteit van gegevens en de systemen waarmee het werk wordt uitgevoerd te borgen. Naast beschikbaarheid en integriteit speelt ook de vertrouwelijkheid van (persoons)gegevens een rol.

Archiefbeleid, managementinformatie, gegevensvernietiging

[3] Zie artikel 4 sub 7 AVG: “een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt; wanneer de doelstellingen van en de middelen voor deze verwerking in het Unierecht of het lidstatelijke recht worden vastgesteld, kan daarin worden bepaald wie de verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen”

Het archiefbeleid van de gemeente Roermond is vastgelegd in de Archiefverordening en het Archiefbesluit Gemeente Roermond. Hierin zijn tevens bepalingen opgenomen omtrent gegevensvernietiging. Deze voorschriften zijn gebaseerd op de Archiefwet. Privacywetgeving en – beleid en de Archiefwet en – besluit moeten in onderlinge samenhang bekeken worden.

Integriteit
Privacy bewust werken en integer zijn raken elkaar. Integer zijn is niet voldoende om te voldoen aan de AVG, maar veilig omgaan met persoonsgegevens vereist een integere houding. In het kader van integriteit leggen nieuwe medewerkers de eed of belofte af en hebben zij een geheimhoudingsplicht.

2. Privacymanagement

Privacy is niet alleen het domein van de automatiseringsafdeling maar van eenieder, hoewel de problematiek van databescherming vaak benaderd wordt vanuit de technische hoek. Dat is te beperkt. De bescherming van privacy is een breed werkterrein: het gaat hierbij bijvoorbeeld om het nemen van technische en organisatorische maatregelen, om het in overeenstemming met de wetgeving brengen van de verwerking van persoonsgegevens, om het maken van afspraken met partijen met wie informatie wordt gedeeld, om de interne communicatie en protocollen, en om voorlichting aan de betrokkenen. De gehele organisatie is betrokken bij de verwerking van persoonsgegevens en dus is het logisch dat de verantwoordelijkheid wordt belegd waar alle lijnen samenkomen: het college, dat doorgaans de verantwoordelijke voor de verwerking is.

Privacy dient geborgd te worden middels een vaste plek in het college/management, met een vaste portefeuillehouder die de tijd, kennis en bestuurskracht heeft om in te grijpen in alle onderdelen van de organisatie en haar processen waar de zorgvuldigheid van persoonsgegevens in het geding is. Een goed privacymanagement vergt goede werkwijzen, geboden en verboden. Het vergt overzicht over de totale keten waarbinnen data van de organisatie rond gaat en het maken van afspraken waarbinnen dit gebeurt. De verwerking van persoonsgegevens moet worden gemonitord en er moet worden ingegrepen als contractspartners hun afspraken niet nakomen. Goed privacy management is geen absolute garantie dat er nooit een datalek of andere calamiteit zal ontstaan. Maar als het gebeurt, kan in ieder geval niemand het verwijt van onbehoorlijk en onrechtmatig bestuur gebruiken.

Om daadwerkelijk te kunnen waarborgen dat privacybescherming ingebed wordt in onze organisatie is het noodzakelijk dat alle medewerkers die persoonsgegevens verwerken deze data goed beheren en het proces gemanaged wordt vanuit een centrale visie. Daarvoor is onderstaand governance model ingericht.

2.1. Verantwoordelijkheid voor naleving AVG en privacybeleid

De bestuursorganen van de gemeente Roermond zijn verantwoordelijk voor de naleving van de AVG en het privacybeleid, ieder voor zover het hun bestuurlijke taken betreft. Zij zijn verantwoordelijk voor het verwerken van persoonsgegevens door de eigen organisatie en aan externe organisaties gemandateerde taken. Voor zover de verwerking van persoonsgegevens gedelegeerd is aan externe organisaties die daarbij ook zelf doel en middelen kunnen bepalen, zijn de bestuursorganen van deze organisaties zelf verantwoordelijke in de zin van de AVG.

Het college en de burgemeester zullen binnen de jaarlijkse planning & control cyclus de gemeenteraad informeren over de risico's en over de getroffen beheersmaatregelen op het gebied van privacy. Daarnaast heeft de raad op 14 juli 2016 besloten aan het Auditcomité

het voeren van periodiek overleg met het college over het onderwerp informatieveiligheid op te dragen.

Op grond van de AVG wordt de uitvoering van het privacybeleid door de Functionaris Gegevensbescherming (hierna: FG) geauditeerd. De FG rapporteert aan het college. Dit doet overigens niet af aan de algemene informatieplicht van het college en de burgemeester afzonderlijk[4].

Het college en de burgemeester melden bijzonderheden ten aanzien van gegevensverwerkingen, te denken valt aan ernstige datalekken, proactief aan de gemeenteraad. Binnen het college wordt een portefeuillehouder aangewezen voor privacy.

2.2. Sturing en monitoring

Proceseigenaren en de verantwoordelijke portefeuillehouder zijn verantwoordelijk voor de zorgvuldige verwerking van persoonsgegevens die binnen hun proces of organisatie plaatsvindt. Zij zijn daarom ook verantwoordelijk voor de monitoring of persoonsgegevens zorgvuldig worden verwerkt en dienen dit zo nodig bij te sturen.

Een belangrijk uitgangspunt in de AVG, waarop de Autoriteit Persoonsgegevens zal gaan handhaven, is accountability: de verantwoordelijke is verantwoordelijk voor de naleving van wetgeving en kan dit aantonen[5] (verantwoordingsplicht).

Om hieraan te kunnen voldoen rapporteren de proceseigenaren - gevraagd en ongevraagd- aan de FG over de realisatie van passende privacy-waarborgen.

Leidinggevenden en medewerkers nemen privacy als onderdeel van hun werkoverleggen op. De organisatie werkt zo actief aan privacy bewustzijn, het opbouwen van kennis bij medewerkers en aan verantwoorde procesuitvoering.

Om het management te ondersteunen zullen experts ingezet worden op het gebied van gegevensverwerking en informatiebeveiliging. Deze experts werken nauw met elkaar samen. In de onderstaande alinea's wordt hun expertise beschreven.

2.3. Functionaris Gegevensbescherming (FG)

Voor onafhankelijk toezicht en controle op de kwaliteit van de uitvoering van de AVG en het privacybeleid heeft de gemeente Roermond een FG aangesteld. Deze functie wordt gepositioneerd binnen het team Concern Control. De FG heeft een onafhankelijke positie in de organisatie. De werkzaamheden die een FG uitvoert hebben een wettelijke grondslag.

De taken van de functionaris zijn, kort samengevat, informeren, adviseren, toezicht houden, bewustwording creëren, en optreden als contactpersoon van de Autoriteit Persoonsgegevens. Het is niet de bedoeling dat de FG de taken op het gebied van bescherming van persoonsgegevens van de proceseigenaren overneemt. De proceseigenaren hebben hun eigen verantwoordelijkheid in het goed omgaan met privacygevoelige gegevens.

De FG van de gemeente Roermond is als volgt te bereiken:

Per post:

[4] Artikelen 169 en 180 lid 2 van de Gemeentewet
[5] Artikel 5 lid 2 AVG

Gemeente Roermond
T.a.v. de Functionaris Gegevensbescherming
Postbus 900
6040 AX Roermond

Per e-mail: huubmulders@roermond.nl

Telefonisch: zie website gemeente Roermond.

De FG ziet er samen met de verantwoordelijke portefeuillehouder op toe dat er een privacy-auditplan wordt ontwikkeld en dat dit wordt uitgevoerd, . Daarnaast voert hij zelfstandig controles uit of laat controles uitvoeren. De FG ziet toe op de wijze van implementatie van maatregelen door proceseigenaren.

De FG treedt op als adviseur op beleidsniveau. De FG heeft, na formeel verzoek, het recht op toegang tot alle informatie en systemen en processen waarin persoonsgegevens een rol (kunnen) spelen. De FG geniet ontslagbescherming en doet zijn werk vrij van last en opdracht. In aanvulling op de wettelijke bepalingen over de FG (artikel 37 tot en met 39 AVG) is een Statuut vastgesteld waarin positie, taken en bevoegdheden van de FG vastgelegd zijn.

2.4. Privacy Officer

De privacy officer (hierna: PO) is het interne aanspreekpunt voor wat betreft de praktische invulling van de gestelde privacy kaders en communiceert en rapporteert met/aan de FG. De privacy officer heeft de volgende hoofdtaken:

- Adviseren over en meewerken aan het beleid/ visie van Roermond op het gebied van privacy;
- Adviseren over en meewerken aan ad-hoc informatievragen over privacy, het verhogen van het privacy-bewustzijn binnen de organisatie en privacy-protocollen en overeenkomsten in de gehele organisatie;
- Volgt de inzichten, wet- en regelgeving en jurisprudentie omtrent privacy;
- Onderhoudt structurele contacten met de privacy officers van ketenpartners en regiogemeenten;
- Adviseert samen met de CISO over de inrichting en veiligheid van de gegevensverwerkingen en de daarbij behorende datasystemen;
- Organiseert dat de organisatie uitvoering geeft aan de actieve informatieplicht richting betrokkenen die zijn opgenomen in een gegevensverwerking en aan de algemene communicatie rondom de privacy. Dit onder verantwoordelijkheid van de proceseigenaren;
- Het bewaken en borgen van de rechten van betrokkenen en de uitvoering van procedures die hiermee verband houden door proceseigenaren;
- Adviseert in geval van beveiligingsincidenten/ datalekken conform de vastgestelde procedure meldplicht datalekken;
- Levert een bijdrage aan control van privacy;
- Heeft oog voor maatschappelijke ontwikkelingen en is in staat een brug te bouwen tussen maatschappelijke ontwikkelingen en privacy-waarborgen;
- Draagt bij aan bewustwording binnen de organisatie.

2.5. Chief Information Security Officer (CISO)

De CISO bevordert en adviseert gevraagd en ongevraagd over de informatiebeveiliging en -veiligheid van de gemeente, verzorgt rapportages over de informatieveiligheidsstatus, controleert of de maatregelen -voortvloeiende uit het informatiebeveiligingsbeleid- worden nageleefd, evalueert de uitkomsten en doet voorstellen tot implementatie c.q. aanpassing van plannen op het gebied van de informatiebeveiliging van de gemeente.

De CISO is procesregisseur voor wat betreft informatiebeveiligingsvragen in de lijn en bij projecten en werkt nauw samen met de PO en de FG.

3. Privacy beleidskader Gemeente Roermond

3.1. Algemeen

De gemeente is verantwoordelijk voor het opstellen, uitvoeren en handhaven van een privacy beleidskader.

Hiervoor gelden onder andere de volgende wettelijke kaders:

- Wet Bescherming Persoonsgegevens (Wbp) (tot 25 mei 2018);
- Vanaf 25 mei 2018: de Algemene Verordening Gegevensbescherming;
- Per datum inwerkingtreding: de Uitvoeringswet AVG[6].

3.2. Taakstelling en uitgangspunten

De gemeente Roermond gaat op een zorgvuldige manier met persoonsgegevens om en respecteert de privacy van betrokkenen. De gemeente houdt zich hierbij aan de volgende uitgangspunten:

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

Transparantie
Het is belangrijk dat betrokkenen erop kunnen vertrouwen dat hun persoonsgegevens zorgvuldig worden verwerkt. Dat vertrouwen wordt gecreëerd door inzichtelijk te maken, door middel van verschillende communicatiekanalen, op welke wijze persoonsgegevens worden verwerkt en beheerd. In uitzonderingsgevallen kan de gemeente Roermond besluiten om geen informatie over de verwerking van persoonsgegevens te verstrekken. Dit kan bijvoorbeeld het geval zijn bij kwesties van openbare orde en veiligheid, zoals bij het vervolgen, voorkomen en opsporen van een strafbaar feit.

Grondslag en doelbinding
Persoonsgegevens worden alleen verwerkt indien hiervoor een wettelijke grondslag bestaat. De gemeente zorgt ervoor dat persoonsgegevens alleen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doelen worden verzameld en verwerkt. Persoonsgegevens worden vervolgens niet verder verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen.

Dataminimalisatie

[6] Op het moment van schrijven van dit privacybeleidskader, begin 2018, is een voorstel uitvoeringswet in behandeling bij de Tweede Kamer.

De gemeente verwerkt alleen de persoonsgegevens die minimaal noodzakelijk zijn voor het vooraf bepaalde doel. De gemeente streeft naar minimale gegevensverwerking. Waar mogelijk worden minder of geen persoonsgegevens verwerkt.

Bewaartermijn
Het bewaren van persoonsgegevens kan nodig zijn om de gemeentelijke taken goed uit te kunnen voeren of om wettelijke verplichtingen te kunnen naleven. Persoonsgegevens mogen echter niet langer worden bewaard dan noodzakelijk is voor het doel waarvoor ze nodig zijn. Dit doel wordt beschreven in verschillende wetten, daarom lopen de bewaartermijnen van persoonsgegevens uiteen. Daar waar er geen wettelijke bepaling is die voorziet in een verplichte bewaartermijn, dient het college een eigen besluit over de bewaartermijn te nemen. Daarnaast geldt de Archiefwet voor het bewaren van papieren en elektronische documenten.

Integriteit en vertrouwelijkheid
De gemeente gaat zorgvuldig om met persoonsgegevens en behandelt deze vertrouwelijk. Zo worden persoonsgegevens alleen verwerkt door personen met een geheimhoudingsplicht. Daarbij zorgt de gemeente voor passende beveiliging van persoonsgegevens. Deze beveiliging is vastgelegd in het informatiebeveiligingsbeleid.

Met dataclassificatie wordt de uitvoering van het privacy beleid ondersteund. De maatregelen die getroffen moeten worden op het gebied van informatiebeveiliging om gegevensbescherming te kunnen borgen, zijn niet voor elk proces en informatiesysteem hetzelfde. Dit is de reden dat het nodig is dat alle processen en informatiesystemen die gegevens verwerken een eigen dataclassificatie hebben. Dataclassificatie heeft als doel om de beschikbaarheid, integriteit en vertrouwelijkheid van het proces en het informatiesysteem formeel te benoemen. Dit maakt inzichtelijk waarom maatregelen genomen moeten worden om de gegevens die verwerkt worden te beschermen. Elke proceseigenaar voorziet de processen en informatiesystemen die onder zijn/haar verantwoordelijkheid vallen van dataclassificatie zoals voorgeschreven in het informatiebeveiligingsbeleid.

Delen van gegevens
In bepaalde gevallen kan het nodig zijn dat persoonsgegevens gedeeld worden. Het delen van persoonsgegevens vindt niet plaats zonder de expliciete toestemming van betrokkene of wettelijke grondslag of wettelijke verplichting.

Ingeval persoonsgegevens gedeeld worden in het kader van samenwerking met externe partijen maakt de gemeente afspraken met de externe partij over de eisen waar een gegevensuitwisseling aan moet voldoen. Deze afspraken zorgen ervoor dat er passende technische en organisatorische maatregelen genomen worden om een op het risico afgestemd niveau van beveiliging te waarborgen.

Subsidiariteit
Voor het bereiken van het doel waarvoor de persoonsgegevens worden verwerkt, wordt inbreuk op de persoonlijke levenssfeer van de betrokken burger zoveel mogelijk beperkt. Bij iedere verwerking wordt daarom gecontroleerd of er een voor de betrokkene minder belastende manier is om de taak uit te voeren.

Proportionaliteit
De inbreuk op de belangen van de betrokkene mag niet onevenredig zijn in verhouding tot een met de verwerking te dienen doel. Bij iedere verwerking wordt daarom gecontroleerd of er niet meer gegevens verwerkt worden dan noodzakelijk voor het uitoefenen van de taak

Privacy by design
Bij de ontwikkeling van producten en diensten is er aandacht voor privacy en wordt er gebruik gemaakt van privacy-verhogende maatregelen (ook wel *privacy enhancing technologies* of PET genoemd).

Privacy by default
Het concept van Privacy by Default verplicht organisaties om de privacy van belanghebbenden te beschermen door de instellingen en functies van de producten of diensten standaard (by default) op de meest privacy vriendelijke stand te zetten.

3.3. Kapstokregeling

Het privacybeleidskader schept een algemeen kader voor de omgang met persoonsgegevens. In paragraaf 3.1 is reeds toegelicht welke wetten ten grondslag liggen aan de in dit beleidskader opgenomen eisen. Er zijn echter ook veel andere wetten die aanvullende eisen stellen aan privacybescherming, zoals de Wet Basisregistratie Personen (BRP), Wet maatschappelijke ondersteuning 2015 (Wmo) en Jeugdwet. Deze bijzondere wettelijke voorschriften worden in dit beleidskader niet nader ingevuld.

Proceseigenaren geven via specifiek uitvoeringsbeleid nadere invulling aan het privacybeleidskader, in samenspraak met de privacy officer.

4. Inbedding binnen de organisatie

4.1. 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. Het register beschrijft alle verwerkingen van persoonsgegevens binnen de gemeente. De volgende zaken worden vastgelegd in het register:

- de naam en de contactgegevens van de verantwoordelijke en eventuele gezamenlijke verantwoordelijken, en, in voorkomend geval, van de vertegenwoordiger van de verantwoordelijke, en van de FG;
- de doeleinden van de gegevensverwerking;
- een beschrijving van de categorieën van betrokkenen en van de categorieën van persoonsgegevens;
- de categorieën van (voorgenomen) ontvangers;
- indien van toepassing, verstrekking van persoonsgegevens aan een derde land of een internationale organisatie;
- indien mogelijk, de beoogde termijnen waarbinnen de verschillende categorieën van gegevens moeten worden gewist;
- de classificatie van de gegevens;
- indien mogelijk, een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen.

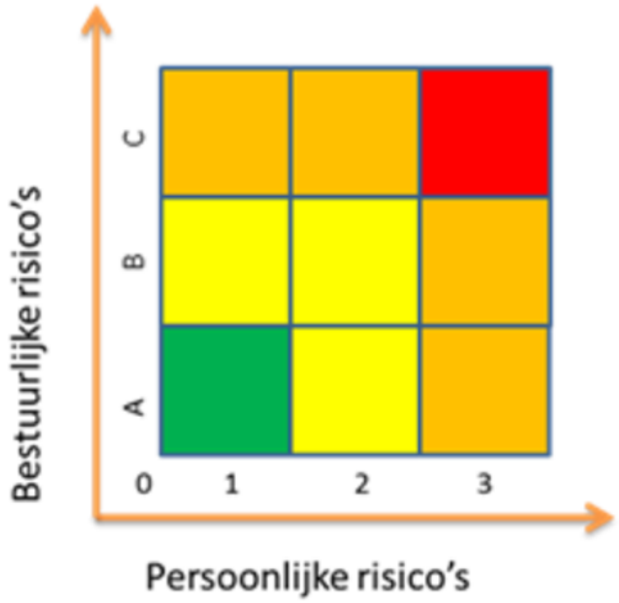
Proceseigenaren melden nieuwe verwerkingen en relevante wijzigingen in bestaande verwerkingen aan de privacy officer. De privacy officer draagt er zorg voor dat deze nieuwe verwerkingen en relevante wijzigingen in het register opgenomen worden.

4.2. Wijze van inrichten gegevensverwerking

Door het cyclische karakter van de te nemen maatregelen en doordat privacy vast op de agenda van bestuur, management en lijnorganisatie is geplaatst, ontstaat een continue proces van veranderen en verbeteren. Privacy management is risicomanagement. De soort verwerking (aard, omvang, context, het doel) en de risico's voor betrokkenen bepalen welke technische en organisatorische maatregelen passend zijn om te kunnen waarborgen en te kunnen aantonen dat verwerkingen conform wet- en regelgeving worden uitgevoerd.

Risico's worden bepaald aan de hand van gegevensbeschermingseffectbeoordeling (ook genoemd "privacy impact assessment" (PIA) of data protection impact assessment (DPIA). Met een gegevensbeschermingseffectbeoordeling worden de effecten en risico's van nieuwe of bestaande verwerkingen beoordeeld op de bescherming van de privacy. Proceseigenaren voeren deze uit wanneer een geautomatiseerde verwerking, een grootschalige verwerking plaatsvindt of wanneer gevoelige gegevens worden verwerkt. Dit geldt in het bijzonder bij verwerkingen waarbij nieuwe technologieën worden gebruikt.

De effecten van een verwerking, zowel profijt als risico's voor personen en de gemeente, worden door middel van een PIA in kaart gebracht en afgewogen op basis van inhoud. De risico's worden door praktische, organisatorische en technische maatregelen beheerst. Met een risicoanalyse (zie afbeelding) wordt de mate van persoonlijk- en bestuurlijk risico in kaart gebracht. Deze vormt het vertrekpunt voor het maken van beleidskeuzes.



De kwaliteit van de omgang met privacy- vraagstukken wordt verhoogd door op verschillende niveaus en vanuit verschillende rollen telkens weer de PDCA-cyclus[7] te doorlopen. Hierdoor ontstaat een evenwichtig privacy- beheersingssysteem.

4.3. Meldplicht datalekken

Waar gehakt wordt vallen spaanders. Ook incidenten zijn helaas niet in alle gevallen te voorkomen. Niet alleen op het gebied van beveiliging (datalekken), maar ook op het gebied van compliance. Denk bijvoorbeeld aan het niet tijdig reageren op een verzoek van betrokkene, het gebruik van gegevens voor een onverenigbaar doel of het langer bewaren van persoonsgegevens dan toegestaan.

[7] De cirkel van Deming: Plan-Do-Check-Act. Continue verbeter cirkel.

Bij een datalek kan gedacht worden aan het kwijtraken van een USB-stick met persoonsgegevens, inbraak door een hacker, maar ook aan onbevoegde autorisaties in een informatiesysteem, het aan iemand toesturen van persoonsgegevens die niet voor de ontvanger zijn bestemd (brief of e-mail) of het zoekraken van een dossier. Ook het intern verwerken van persoonsgegevens door personen die hier niet bevoegd toe zijn vormt een datalek.

Indien een datalek of een vermoeden van een datalek zich voordoet dient de gemeente snel en effectief te handelen. Naast de eigen verantwoordelijkheid die de gemeente Roermond als overheid hierin heeft is zij op grond van wetgeving verplicht een datalek zonder onredelijke vertraging te melden bij de Autoriteit Persoonsgegevens tenzij het niet waarschijnlijk is dat de inbreuk een risico inhoudt voor de rechten en vrijheden van natuurlijke personen. Een melding moet indien van toepassing[8] ook onverwijld aan betrokkenen worden gedaan.

Om aan de wet te kunnen voldoen hanteert de gemeente Roermond een vastgestelde interne procedure die hierop aansluit. Deze procedure is gericht op het snel en zorgvuldig kunnen afhandelen van incidenten en deze zodanig te kunnen documenteren dat achteraf de betrachte zorgvuldigheid kan worden aangetoond. Onderdeel van deze procedure vormt evaluatie van geconstateerde datalekken om incidenten in de toekomst waar mogelijk te voorkomen.

Met externe partijen en opdrachtnemers die persoonsgegevens verwerken zijn afspraken gemaakt hoe te handelen in geval van een datalek. Het melden van een (vermoedelijk) datalek door betrokkenen is mogelijk via de procedures zoals beschreven op de website van de gemeente Roermond. Ook deze meldingen worden, waar nodig, door de privacy officer gemeld bij de Autoriteit Persoonsgegevens. De Autoriteit Persoonsgegevens is bevoegd om datalekken te beboeten en dwingende adviezen te geven ter verbetering van de omgang met persoonsgegevens.

4.4. Convenanten, verwerkersovereenkomsten en geheimhoudingsverklaringen

Met het oog op de bescherming van privacy in gevallen waarin de gemeente samenwerkt en waarbij verwerking van persoonsgegevens plaatsvindt worden convenanten, verwerkersovereenkomsten en geheimhoudingsverklaringen afgesloten. Proceseigenaren dienen de eisen omtrent gegevensverwerking te borgen in contracten. Hoe er afspraken worden gemaakt met externe partners, is sterk afhankelijk van de positie in de informatieketen en de aard van de samenwerking. Er kan sprake zijn van een samenwerking tussen mede- verantwoordelijken, opdrachtverstrekking aan verwerkers , opdrachtverstrekking aan externen niet zijnde verwerkers, ingehuurde medewerkers en medewerkers die werkzaam zijn voor een externe partij. De privacy officer ondersteunt proceseigenaren hierin.

Het verlenen van opdrachten aan derden, verwerkers, brengt risico's met zich me op het gebied van gegevensverwerking en informatieveiligheid. De bestuursorganen van de gemeente Roermond die derden opdracht geven persoonsgegevens namens hen te verwerken, blijven verantwoordelijk voor deze verwerking. Het aangaan van verwerkersovereenkomsten geeft de mogelijkheid erop toe te zien dat ook door verwerkers zorgvuldig omgegaan wordt met persoonsgegevens en een passende bescherming gewaarborgd is.

[8] Artikel 33 AVG

Om te borgen dat er verwerkersovereenkomsten aangegaan worden die voldoen aan wettelijke eisen is een model verwerkersovereenkomst vastgesteld. Het aangaan van verwerkersovereenkomsten vormt, waar toepasselijk, bovendien vast onderdeel van het inkoopproces.

4.5. Cameratoezicht in gemeentelijke gebouwen

In gemeentelijke gebouwen wordt om reden van veiligheid van medewerkers en bezoekers en ter bescherming van eigendommen van de gemeente en van bezoekers, toezicht middels het gebruik van camera's gehouden. Dit is een vorm van verwerking van persoonsgegevens die onderworpen is aan de regels van de Wet bescherming persoonsgegevens. De Autoriteit Persoonsgegevens heeft beleidsregels opgesteld waaraan het gebruik van camera's in gemeentelijke gebouwen is gebonden.

De gemeente heeft een protocol vastgesteld waarin het gebruik van camera's wordt geregeld alsmede een protocol waarin de rechten van degenen die aan cameratoezicht zijn onderworpen zijn geregeld. Op de gemeentelijke website kunnen burgers een formulier vinden waarmee de mogelijkheid wordt geboden om camerabeelden bij een gerechtvaardigd belang in te kunnen zien.

4.6. Bewustwording

Een ketting is zo sterk als haar zwakste schakel. Verantwoord en bewust gedrag van iedere medewerker die in aanraking komt met persoonsgegevens is dan ook essentieel om te kunnen waarborgen dat privacywetgeving wordt nageleefd. Het is van groot belang dat medewerkers die werken met persoonsgegevens weten wat hun verantwoordelijkheid is en hoe zij zorgvuldig om dienen te gaan met persoonsgegevens. Zij dienen in staat te zijn om te beoordelen welke gegevens nodig zijn voor het uitvoeren van de werkprocessen. Er dienen niet te weinig maar ook niet te veel gegevens te worden verwerkt[9].

Beleid en maatregelen alleen zijn niet voldoende om risico's op het gebied van de verwerking van persoonsgegevens uit te sluiten. Privacy bewustzijn wordt daarom binnen de gemeente Roermond voortdurend aangescherpt, zodat kennis van risico's wordt verhoogd en veilig en verantwoord gedrag wordt aangemoedigd.

De cultuur binnen de organisatie in zijn geheel moet op een "bewust bekwaam" niveau van omgaan met persoonsgegevens worden gebracht. Er worden alleen gegevens verwerkt op basis van "need to know" en niet op basis van "nice to know", waarbij voor wat betreft de laatste categorie geen persoonsgegevens worden verwerkt.

Om hiervoor zorg te dragen voorziet het college in faciliteiten voor bewustwording en training.
Proceseigenaren zorgen er voor dat informatie over gegevensbescherming en informatieveiligheid herhaaldelijk onder de aandacht wordt gebracht van leidinggevenden en medewerkers. Zij worden hierin bijgestaan door FG, CISO en privacy officer. Medewerkers worden getraind in privacy-bewust functioneren door middel van presentaties, workshops en trainingen en het altijd voorhanden hebben van een aanspreekpunt.

5. Privacyservices

5.1. Rechten

[9] Zie artikel 5 lid 1 sub c AVG

Op grond van de AVG krijgen betrokkenen nieuwe rechten en hun bestaande rechten worden uitgebreid. Organisaties die persoonsgegevens verwerken krijgen meer verplichtingen. De nadruk ligt op de verantwoordelijkheid van organisaties om te kunnen aantonen dat zij zich aan de wet houden (accountability). Onderdeel hiervan vormt het op transparante wijze inrichten van de rechten van de betrokkene. Hierbij wordt gebruik gemaakt van het navolgende kader:

Wet openbaarheid van bestuur (Wob)

Via de Wob (en straks wellicht de Wet Open Overheid) kan een verzoek om informatie ingediend worden bij de gemeente. Bij beoordeling van het verzoek bekijkt de gemeente altijd of het antwoord geen inbreuk maakt op de persoonlijke levenssfeer van betrokkenen.

Wet hergebruik van overheidsinformatie

Op grond van de Wet hergebruik van overheidsinformatie dient de gemeente in voorkomende gevallen op verzoek overheidsinformatie te verstrekken voor hergebruik. Bij beoordeling van het verzoek bekijkt de gemeente altijd of het antwoord geen inbreuk maakt op de persoonlijke levenssfeer van betrokkenen.

Rechten van betrokkenen (artikel 13 t/m 20 AVG)

In de AVG zijn de volgende rechten van betrokkenen opgenomen:

- *Informatieplicht (artikel 13 en 14 AVG)*

  De gemeente informeert betrokkenen over het verwerken van persoonsgegevens. Wanneer betrokkenen persoonsgegevens aan de gemeente geven, dienen zij op de hoogte te worden gesteld over de manier waarop de gemeente met persoonsgegevens om zal gaan. Dit kan bijvoorbeeld via een vermelding op een aanvraagformulier gebeuren, of op andere algemeen gangbare wijze (informatiefolder o.d.). 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, dus buiten de betrokkene om, dan dient betrokkene daarover geïnformeerd te worden op het moment dat deze voor de eerste keer worden verwerkt.

- *Inzagerecht (artikel 15 AVG)*:

  De betrokkene heeft het recht om te informeren of zijn persoonsgegevens worden verwerkt. Als dat het geval blijkt, heeft hij recht op uitleg welke persoonsgegevens het betreft en op welke manier deze gegevens worden verwerkt. Ook heeft hij recht op inzage en een kopie van zijn persoonsgegevens (zie nader artikel 20 AVG). De gemeente kan verlangen dat de betrokkene zich op adequate wijze identificeert. Het recht van inzage is mede bedoeld om uitoefening van het recht op rectificatie, het recht op gegevens wissen en beperking van de verwerking mogelijk te maken. Een verzoek om dit recht uit te oefenen kan bijvoorbeeld via het invullen van een formulier gebeuren, dat bij voorkeur toegankelijk is middels het gebruik van DigiD.

- *Recht op rectificatie (artikel 16 AVG)*

Als verwerkte persoonsgegevens onjuist of onvolledig zijn kan de betrokkene aan de gemeente verzoeken deze te laten corrigeren of aanvullen. De gemeente en eventuele externe partijen die in opdracht van de gemeente persoonsgegevens verwerken moeten onverwijld alle redelijke maatregelen nemen om ervoor te zorgen dat onjuiste persoonsgegevens worden gerectificeerd. Het is daarbij irrelevant wiens fout het is dat de persoonsgegevens onjuist zijn.

- *Recht op gegevenswissing, recht op "vergetelheid" (artikel 17 AVG)*

  Betrokkenen hebben het recht om de gemeente te verzoeken bovenmatige persoonsgegevens te wissen. Er is sprake van overtollige persoonsgegevens in de volgende gevallen:

  - Als persoonsgegevens niet langer nodig zijn voor de doeleinden waarvoor zij verwerkt worden;
  - Als de betrokkene zijn toestemming voor de verwerking op valide gronden intrekt;
  - In geval van een gegrond bezwaar en er is geen zwaarwichtig belang voor de verwerking;
  - Als de persoonsgegevens onrechtmatig verwerkt zijn;
  - Als de wet dwingt tot verwijdering;
  - Als gegevens van kinderen zijn verzameld in het kader van diensten van de informatiemaatschappij (bijv. website, app).

  De gemeente is in een dergelijk geval verplicht om zo snel mogelijk aan het verzoek om gegevenswissing gehoor te geven, tenzij er sprake is van een uitzondering zoals opgenomen in artikel 17 lid 3 AVG.

- *Recht op beperking van de verwerking (artikel 18 AVG)*

  Betrokkene mag vragen om beperking van de verwerking in de volgende gevallen:

  - De juistheid van de gegevens wordt door betrokkene betwist;
  - De gegevens worden onrechtmatig verwerkt maar de betrokkene niet wil dat de gegevens worden verwijderd;
  - De doeleinden zijn vervallen, maar betrokkene heeft de gegevens nog nodig voor de uitoefening/ verdediging van enig recht in rechte;
  - In geval van een lopende bezwaarprocedure.

  Als hier sprake van is, mag tijdelijk geen andere verwerkingshandeling plaatsvinden dan opslag, tenzij:

  - De betrokkene daar toestemming voor geeft;
  - Dit nodig is voor de uitoefening/ verdediging van enig recht in rechte;
  - Dit nodig is om gewichtige redenen van algemeen belang.

  De betrokkene dient vervolgens geïnformeerd te worden voordat de blokkade opgeheven wordt.

- *Recht van bezwaar (artikel 21 AVG)*

  Betrokkenen hebben het recht om bezwaar te maken tegen de verwerking van hun persoonsgegevens onder de volgende voorwaarden:

- er is sprake is van verwerking op basis van een publiekrechtelijke taak van een bestuursorgaan of;
- er is sprake is van een verwerking op basis van een gerechtvaardigd belang (inclusief profilering)

en betrokkene kan aantonen dat er sprake is van specifieke persoonlijke omstandigheden die het maken dat de belangenafweging van de verwerking in zijn geval anders zou moeten uitpakken.

Als aan deze voorwaarden voldaan is dient de gemeente te stoppen met verwerken tenzij:

- De gemeente “dwingende wettige redenen” heeft die prevaleren boven de belangen van de betrokkene;
- De persoonsgegevens nodig zijn voor uitoefening/ verdediging van enig recht in rechte.

Als de verwerking plaatsvindt in het kader van wetenschappelijk of historisch onderzoek en statistiek geldt het recht van bezwaar niet als de verwerking geschiedt in het kader van algemeen belang.

- *Recht op overdraagbaarheid van gegevens, dataportabiliteit (artikel 20 AVG)*

  De betrokkene heeft desgevraagd het recht om zijn persoonsgegevens te verkrijgen in een gestructureerd, gangbaar en machine-leesbaar format. Hij mag deze gegevens overdragen aan een andere verantwoordelijke zonder daarbij te worden gehinderd door de eerste verantwoordelijke.

  Waar mogelijk heeft de betrokkene er recht op dat een verantwoordelijke rechtstreeks zijn persoonsgegevens doorstuurt naar de nieuwe verantwoordelijke.

- *Recht om niet te worden onderworpen aan een uitsluitend op geautomatiseerde verwerking gebaseerd besluit (artikel 22 AVG)*

  De betrokkene heeft het recht niet te worden onderworpen aan een uitsluitend op geautomatiseerde verwerking (waaronder profilering), gebaseerd besluit waaraan voor hem rechtsgevolgen zijn verbonden of dat hem anderszins in aanmerkelijke mate treft, behalve als er sprake is van de in artikel 22 AVG genoemde gevallen.

5.2. Uitoefening rechten betrokkene

Om gebruik te maken van zijn/haar rechten kan de betrokkene een verzoek indienen. Naar aanleiding van het verzoek kan de gemeente aanvullende informatie opvragen om de identiteit van de betrokkene vast te kunnen stellen. Op de gemeentelijke website wordt een toelichting geplaatst over de betreffende procedure, zodat betrokkenen effectief hun rechten uit kunnen oefenen. Als het verzoek wordt afgewezen is er de mogelijkheid om bezwaar te maken bij de gemeente, of een klacht in te dienen bij de Autoriteit Persoonsgegevens (AP). Hierover zal betrokkene geïnformeerd worden.

5.3. Klachten

In het contact met de gemeente gaat wel eens wat mis. Een burger, bedrijf of instelling kan zich onheus bejegend voelen. Dan is het goed om te weten, dat ieder op grond van de Algemene wet bestuursrecht (Awb) het recht heeft een klacht in te dienen over de wijze waarop een gemeentelijk bestuursorgaan of iemand die in dienst van de gemeente werkzaam is, zich jegens hem of een ander heeft gedragen.

Hoofdstuk 9 van de Awb regelt de behandeling c.q. het buiten behandeling laten van klachten. In aanvulling daarop kan er een klachtenregeling zijn. De klachtenregeling binnen de gemeente Roermond is vastgelegd in de Verordening interne klachtadviescommissie 2010. Deze verordening is terug te vinden op www.overheid.nl onder lokale wet- en regelgeving.

Indien de klachtenprocedure in relatie staat tot de verwerking van persoonsgegevens zal de behandelend ambtenaar van de klachtadviescommissie afstemming zoeken met de FG.

6. Schema verantwoordelijkheden en borging

In onderstaand schema is samengevat hoe de verantwoordelijkheden en de borging van het privacybeleid binnen de gemeente Roermond worden georganiseerd.

Verantwoordelijkheid	**Wie en hoe**
Vaststellen privacy beleid	Het bestuur van de gemeente Roermond heeft het beleid vastgesteld en bevordert de beschikbaarheid van voldoende middelen om privacybescherming passend te waarborgen.
Beheer van privacy beleid	De privacy officer beheert het beleid, in samenspraak met de FG en portefeuillehouder privacy. De FG rapporteert aan het college over de voortgang en de kwaliteit van de uitvoering, en doet aanbevelingen voor verdere optimalisering. Waarborg voor optimalisering is het hanteren van de PDCA-cyclus.
Uitvoering van privacy beleid	Er is een portefeuillehouder privacy aangewezen. Deze is verantwoordelijk voor uitvoering van het privacy beleid alsmede voor controle op de naleving van afspraken. Proceseigenaren zijn verantwoordelijk voor implementatie van het privacybeleidskader binnen hun proces~~,~~ en voor uitvoering van de hierin opgenomen normen. Zij rapporteren hierover gevraagd en ongevraagd aan de FG.
Ontwikkelen en uitvoeren van thematisch beleid	De portefeuillehouder privacy ziet toe op de ontwikkeling en uitvoering van themagericht privacy beleid (BRP, Participatie, Jeugd etc.) door proceseigenaren. Hieronder wordt met name ook verstaan: aantoonbare concretisering van beleid in praktische waarborgen, zodat ook op operationeel niveau structureel sprake is van behoorlijke en zorgvuldige verwerking van persoonsgegevens in overeenstemming met de wet. De proceseigenaar krijgt hierbij ondersteuning van de privacy officer.
Bestuurlijke verantwoording	Jaarlijks legt het college verantwoording af aan de gemeenteraad over de risico's en beheersmaatregelen.
Toezicht	De gemeente Roermond heeft een Functionaris Gegevensbescherming (FG) aangesteld die toeziet op de naleving van privacy- wet- en regelgeving en privacybeleid. De FG kan aan de bestuursorganen rapporteren en onderhoudt de contacten met de Autoriteit Persoonsgegevens. De positie en taken van de FG zijn

Verantwoordelijkheid	Wie en hoe
	toegelicht in artikel 38 en 39 AVG en verder uitgewerkt in het Statuut Functionaris Gegevensbescherming.
Privacy- auditplan	De FG ziet er samen met de verantwoordelijke portefeuillehouder op toe dat er een privacy- auditplan wordt ontwikkeld en dat dit wordt uitgevoerd. Dit plan wordt jaarlijks opgesteld en is in lijn met het Raamwerk privacy-audit van de Autoriteit Persoonsgegevens. De PDCA-cyclus wordt hierop toegepast.
Risico gedreven aanpak	Vertrekpunt voor het maken van beleidskeuzes is de PIA. In samenwerking met de privacy officer en na advies van de FG brengen proceseigenaren de mate van persoonlijk en bestuurlijk risico in kaart. De FG ziet in overleg met de proceseigenaren toe op de controle van de uitvoering van de op basis van PIA's voorgestelde maatregelen. De risico's worden door praktische, organisatorische en technische maatregelen beheerst en volgens de PDCA-cyclus geborgd.
Register van verwerkingen	Het college is verantwoordelijk voor het aanleggen van een register van verwerkingen. Proceseigenaren melden nieuwe verwerkingen en relevante wijzigingen in bestaande verwerkingen aan de privacy officer. De privacy officer draagt er zorg voor dat deze verwerkingen en wijzigingen in het register opgenomen worden.
Meldplicht datalekken	De verantwoordelijkheden t.a.v. de meldplicht datalekken zijn vastgelegd in de interne procedure meldplicht datalekken.
Convenanten, verwerkersovereenkomsten en geheimhoudingsverklaringen	Daar waar samengewerkt wordt met externe partijen, of aan externe partijen opdracht gegeven wordt om persoonsgegevens te verwerken zijn de proceseigenaren verantwoordelijk voor het aangaan van convenanten, verwerkersovereenkomsten en geheimhoudingsverklaringen. Zij worden hierin ondersteund door de privacy officer.
Bewustwording	De FG en privacy officer zien er – samen met de proceseigenaren – op toe dat medewerkers regelmatig getraind worden en dat actief ingezet wordt op bewustmaking ten aanzien van privacy. Het college voorziet in faciliteiten voor bewustwording en training.
Privacyservices	Proceseigenaren zijn verantwoordelijk voor correcte en transparante afwikkeling van de verzoeken van betrokkenen. Zij rapporteren hierover - per verzoek - over verzoek en afhandeling aan de FG. De privacy officer ondersteunt proceseigenaren in eerbiediging van de rechten van betrokkenen.
Klachten	De interne klachtencoördinatoren zijn verantwoordelijk voor de behandeling van klachten. Indien de klachtenprocedure in relatie staat tot de verwerking van persoonsgegevens wordt afstemming gezocht met de FG.

7. Beheer en onderhoud

Er bestaat niet alleen een wettelijke verplichting om een passend gegevensbeschermingsbeleid te hebben en uit te voeren, maar ook om dit beleid te evalueren en waar nodig te actualiseren[10].

Binnen de gemeente Roermond is de privacy officer eigenaar van het privacybeleidskader en daarmee verantwoordelijk voor het beheer en onderhoud ervan.

Het privacybeleidskader wordt eens per twee jaren geëvalueerd, waarbij in ieder geval de volgende aspecten beoordeeld zullen worden: inhoud, uitvoerbaarheid, invoering en werking. De FG wordt geïnformeerd op basis van deze evaluatie. Indien daartoe aanleiding bestaat wordt het privacybeleidskader geactualiseerd.

Vastgesteld door het college van burgemeester en wethouders d.d. 24 april 2018.

[10] Zie artikel 24 lid 1 en 2 AVG