Privacybeleidskader

Mensgerichte digitalisering



Gemeente Raalte

Gemeente Raalte

Inhoud

1. Inleiding **3**

2. Visie **4**

2.1 Mensgerichte digitalisering 4

2.2 We gaan mee met de tijd 4

2.3 Eigenaarschap 4

2.4 De norm 5

2.5 Lerende organisatie 5

3. Doel en missie **6**

3.1 Doel 6

3.2 Missie 6

4. Eigenaarschap **7**

4.1 Eigenaarschap in de eerste lijn 7

4.2 Eigenaarschap in de tweede lijn 7

4.3 Eigenaarschap in de derde lijn 8

5. Behoorlijk bestuur met data **10**

5.1 Op zoek naar de balans 10

5.2 Werkprogramma Privacy en jaarplannen 10

5.3 De Schaal van Erg 11

5.4 Data Protection Impact Assessments (DPIA) 11

6. Privacyrechten en incidentenmanagement **13**

6.1 AVG/Wpg-verzoeken 13

6.2 fg@dowr.nl 13

6.3 Datalekken 13

7. Handhavingsbeleid **14**

7.1 Handhaving in de eerste en tweede lijn 14

7.2 Handhaving in de derde lijn 14

7.3 Handhaving in de vierde lijn 15

8. Beleidsevaluatie **16**

8.1 Periodiek onderzoek naar doelmatigheid en doeltreffendheid 16

8.2 Onderzoek bij ontbreken van FG-verslagen 16

Gemeente Raalte

1. Inleiding

Voor u ligt het privacybeleidskader. Dit document vormt het fundament onder de beleidsvoering omtrent de Algemene Verordening Gegevensbescherming (AVG) en aanverwante wetgeving. De gemeenteraad van Raalte heeft, samen met gemeente Deventer en gemeente Olst-Wijhe, in de i-Visie een richtinggevend kader vastgesteld met betrekking tot digitalisering en de informatievoorziening. Dit privacybeleidskader is hierop een aanvulling en borgt mensgerichte digitalisering.

In ons denken en handelen gaat de aandacht meestal naar de 'uiterlijkheden' van digitalisering. Denk aan cloudoplossingen, smart city-toepassingen, inzet van algoritmes, gegevensdeling in samenwerkingsverbanden, profiling, mobiel internet, thuiswerken, bodycams, drones, en afhankelijkheid van Amerikaanse big tech-bedrijven.

De privacywetgeving is neutraal ten opzichte van die uiterlijkheden. Iets is niet bij voorbaat goed of fout. In plaats daarvan draait het om wat we ermee doen – het achterliggende proces. De gemeente heeft de flexibiliteit om zich te organiseren op de manier die wij het meest wenselijk achten zolang doelgroepen – met name inwoners – er verzekerd van kunnen zijn dat de gemeente integer handelt.

Dit document stelt het volgende vast:

- de bestuurlijke visie op gegevensbescherming;
- rollen en verantwoordelijkheden;
- managementafspraken over risicosturing;
- toetsing van maatregelen;
- afspraken over transparantie;
- en de manier waarop de gemeente faciliteert dat inwoners en andere doelgroepen hun rechten volgens de AVG kunnen uitoefenen.

Dit kader is tegelijkertijd ook de kapstok waaraan AVG-oplossingen worden opgehangen, zoals een procedure datalekken. Uiteindelijk vormen het privacybeleidskader en de daaraan gekoppelde regelingen het totale privacybeleid van de organisatie.

Door dit privacybeleidskader vast te stellen, ons hiernaar te organiseren en het daadwerkelijk uit te voeren, hebben wij onze basis op orde. Er ontstaat *governance*. Het biedt ons het morele kompas om op het informationele vlak de goede dingen te doen en de goede dingen *goed* te doen.

Gemeente Raalte

2. Visie

2.1 Mensgerichte digitalisering

De gemeente Raalte is een organisatie waaraan onze inwoners met recht informatie over zichzelf kunnen toevertrouwen. We helpen ze waar dat nodig is, dragen zorg voor leefbaarheid en veiligheid, behartigen hun belangen in onze taakuitoefening en staan op een passende manier met hen in verbinding. Dat betekent ook dat we begrijpen wanneer we ze met rust moeten laten.

Mensgerichte digitalisering staat voor het daadwerkelijk kunnen aanhouden van de menselijke maat. We zijn géén domme bureaucratie. Onze gemeente creëert geen kafkaëske toestanden. We kunnen niet 100% voorkomen dat iemand door een vergissing onheus bejegend wordt, maar je kunt altijd op ons terugvallen.

We betrekken inwoners bij keuzes en dilemma's. Onze oplossingen zijn geen black box maar we kunnen het uitleggen, en houden rekening met de wensen en behoeften van onze doelgroepen. Kortom, we waarborgen dat onze informatievoorzieningen ten dienste van de mens staan in plaats van andersom.

2.2 We gaan mee met de tijd

Als gemeente Raalte gaan we mee met de tijd, de maatschappij en technologische ontwikkelingen. We zien hierin kansen om nog meer het goede te doen. Met behulp van online dienstverlening is de gemeente bereikbaarder geworden, is informatie sneller uitgewisseld en beschikken we makkelijker over stuurinformatie. Dat helpt ons in onze taakuitoefening en draagt bij aan de kwaliteit van bestuurlijke besluitvorming.

Maar we zien ook uitdagingen. Met name dat we iemand verkeerd in onze systemen hebben staan of over die persoon verkeerde conclusies trekken. Als dat gebeurt zijn we juist niet mensgericht. We maken van leven in Raalte dan iets onaangenaams. Praktijken zoals een toeslagenaffaire op gemeentelijk niveau willen we voorkomen. In het bijzonder hebben we rekening te houden met de mensen die minder digitaal vaardig zijn.

Dat betekent dat we ons hierop moeten aanpassen. Het volstaat niet meer dat we ons richten op *wat* we doen (openbare orde & veiligheid, maatschappelijke ondersteuning, wonen & omgeving, belastingheffing, enzovoorts), maar ook *hoe* we dat (gedigitaliseerd) organiseren.

Veel van de dingen die we doen, doen we in samenwerking met anderen. Gemeente Raalte staat in verbinding met andere gemeenten en ketenpartners zoals de politie en zorginstellingen, uitvoeringsorganisaties en uiteenlopende dienstverleners in de ICT-sector.

2.3 Eigenaarschap

We zijn eindverantwoordelijk voor die gegevensverwerkingen waarvan bij wet of gemeentelijke regeling is geregeld dat het bestuurlijk eigenaarschap berust bij de raad, de burgemeester of het college. Ook als we taken uitbesteden.

'Eigenaarschap' is het sleutelwoord. En dat is niet alleen van toepassing op het bestuur. Gemeente Raalte zijn we allemaal. Het gaat erom dat iedereen verantwoordelijkheid néémt, vanuit onze verschillende rollen en verantwoordelijkheden.

- Het college en de directie sturen aan de hand van SMART-geformuleerde regieafspraken op de kwaliteit en mensgerichtheid van onze informatievoorzieningen.
- De raad zet de grote lijnen uit (wat voor gemeente willen we zijn in de toekomst), maakt die volwassenwording financieel mogelijk en bewaakt het bereiken van mijlpalen.
- Alle medewerkers zijn medeverantwoordelijk voor betrouwbare, transparante en veilige informatieverwerking.

- Supportfuncties vanuit (o.a.) privacy, informatieveiligheid, informatiebeheer, informatiemanagement, communicatie en ICT dragen bij vanuit ieders eigen invalshoek.
- Toezichtfuncties bewaken en handhaven op bestuursniveau de doelmatigheid en doeltreffendheid van de gemeentelijke informatiebeleidsvoering.

We brengen eigenaarschap in de praktijk door verantwoord met data om te gaan. Mensgerichte digitalisering is vooral iets dat we moeten *doen*. Het moet in ons DNA zitten. Dat vraagt kennis en vaardigheden.

2.4 De norm

De volgende normen voor mensgerichte digitalisering en het kwaliteitsniveau dat we hebben te bereiken, zijn voor ons van toepassing:

1. De Algemene Verordening Gegevensbescherming (AVG) is onze maatstaf voor behoorlijke en zorgvuldige informatieverwerking in de bestuurlijke sfeer.
2. De Wet Politiegegevens is onze maatstaf voor behoorlijke en zorgvuldige informatieverwerking in de justitiële sfeer.
3. Ook wordt waar nodig rekening gehouden met de Verordening Artificiële Intelligentie (AI Act).

2.5 Lerende organisatie

Mensgerichte digitalisering bereik je niet van de ene op de andere dag. Maar we zetten in de komende tijd stappen op het gebied van professionalisering en borging zodat we in 2030 op het benodigde kwaliteitsniveau zitten.

We hebben dan alle aspecten van de gemeentelijke bedrijfsvoering doorgelicht, inclusief uitbestede taken en informatiedeling in samenwerkingsverbanden. En bovenal hebben wij tegen die tijd voorzien in passende maatregelen om onze doelgroepen en onszelf, te beschermen tegen reële risico's.
Nieuwe initiatieven, bijvoorbeeld op het gebied van datagedreven werken of smart-city-toepassingen, worden met passende waarborgen omkleed.

We dragen ook zorg voor de culturele kant en de vereiste kennis, wat per organisatieonderdeel zal verschillen. Fouten gaan we zo goed als mogelijk tegen, maar kunnen we nooit helemaal voorkomen. Daarnaast gaan zich ongetwijfeld problemen voordoen die we niet hebben voorzien.
Eén cultuuraspect staat daarom voorop: Raalte omarmt het concept van *just culture*: zelfs de grootste fout kun je veilig melden. Waar mensen werken worden fouten gemaakt. Van incidenten onderzoeken we de oorzaken, om ons daarin te verbeteren. Gemeente Raalte is een lerende organisatie.

Gemeente Raalte

3. Doel en missie

3.1 Doel

Het doel van dit beleidskader is de vaststelling van rollen en verantwoordelijkheden voor behoorlijk bestuur met data, waarbij de mens centraal staat.

In de missieformulering hierna geven we, in aansluiting op de EU-normstelling, aan dat het Privacybeleidskader de bescherming van *alle* rechten en vrijheden waarborgt (publieke waarden), waaronder het recht op bescherming van privéleven, maar ook bijvoorbeeld het recht op waardigheid en het recht op veiligheid.

Dit beleidskader is erop gericht om deze belangen naar evenredigheid tegen elkaar af te wegen, ook rekening houdend met het algemeen belang dat we als gemeenten dienen.

Het Privacybeleidskader is van toepassing op alle vormen van gemeentelijk functioneren waarvoor informatie over personen wordt verwerkt (verwerking persoonsgegevens). Ook de ICT is daar onderdeel van. Het maakt daarbij niet uit of we taken zelf uitvoeren, laten uitvoeren of onze ICT uitbesteden. Daar waar de gemeente bij wet of gemeentelijke verordening eindverantwoordelijk is, is dit beleid van toepassing. Bepalend is de aanwijzing van het bevoegde bestuursorgaan of bijvoorbeeld de verantwoordelijkheid van de gemeente als werkgever.

3.2 Missie

Met dit beleidskader waarborgen wij de bescherming van personen over wie de gemeente gegevens verwerkt of laat verwerken (bescherming van rechten en vrijheden). Tegelijk verzekeren wij op deze manier de beschikbaarheid, kwaliteit en doorstroming van informatie waar dat nodig is. We benutten de mogelijkheden van digitalisering, maar onderkennen ook de keerzijden ervan.

Dit document is gericht op de garanties van rechtmatige gegevensverwerking en doelmatige en doeltreffende beheersing van risico's. Dit is in zoverre apolitiek dat oplossingsgerichtheid voorop staat. Wij laten ons leiden door objectieve beoordeling van risico's. Een en ander volgens de normstelling door de Europese Unie via, onder meer, de AVG en de AI Act.

We betrachten op alle niveaus het teamspel dat ervoor nodig is om te voorzien in passende waarborgen. Hiervoor stellen wij het Werkprogramma Privacy op. Het werkprogramma helpt ons bij de duurzame vormgeving van de digitale leefomgeving en behoorlijk bestuur met data.

Wij verwerken of laten geen persoonsgegevens verwerken zonder passende waarborgen. Afspraken op dit vlak zijn SMART opgesteld en leggen wij vast. Het gemeentebestuur kan op deze manier steeds verantwoording afleggen over beleid en maatregelen, zowel bestuurlijk, maatschappelijk als juridisch.

Gemeente Raalte

4. Eigenaarschap

4.1 Eigenaarschap in de eerste lijn

Met de vaststelling van dit Privacybeleidskader hernieuwt het gemeentebestuur de opdracht tot behoorlijke en zorgvuldige verwerking van persoonsgegevens. Tevens onderschrijft het gemeentebestuur haar eigen aandeel hierin. Dit naar gelang de verantwoordelijkheden naar Europees en Nederlands publiekrecht – of naar de maatstaven van het privaatrecht zoals goed werkgeverschap.

Voor de beleidsvoering betekent dit dat de bestuursorganen college, burgemeester en raad sturing geven en eindverantwoordelijk zijn conform ieders taakstelling. Binnen het college is er een portefeuillehouder voor digitalisering. Daarnaast blijven burgemeester en wethouders volgens ieders eigen portefeuille verantwoordelijk voor de kwaliteit van gemeentelijke taakuitoefening en rechtsbescherming. Dit betekent dus ook de bescherming van personen bij de verwerking van persoonsgegevens.

De algemeen directeur/gemeentesecretaris is belast met de uitvoering van het privacybeleid, op basis van het Werkprogramma Privacy en bijbehorende begroting. De begroting betreft de algemene middelen voor privacybeleidsvoering, met name de bekostiging van 2e- en 3e lijn support.

Binnen het MT verdeelt de algemeen directeur taken over de proceseigenaren van de gemeente, de domeinmanagers. Proceseigenaren voeren in feitelijke zin de regie over de uitvoering van taken conform het Privacybeleidskader en het bestaan van een volwassen cultuur binnen gemeentelijke domeinen. Dit is nadrukkelijk afgesproken in managementafspraken en is – niet anders dan financiën of HRM – structureel aandachtspunt in het MT-overleg.
Daar waar taken zijn uitbesteed aan dienstenleveranciers of uitvoeringsorganisaties, waarborgen de proceseigenaren aan de hand van vastgelegde afspraken dat voldaan wordt aan de AVG en andere kaders op het gebied van gegevensbescherming.
Bij deelname in een gemeenschappelijke regeling en andere samenwerkingsverbanden zorgen we ervoor dat we onze AVG-belangen kunnen behartigen. Daartoe voorziet de proceseigenaar de gemeentebestuurder van de benodigde sturingsinformatie.

Bestuurders, directie en proceseigenaren koersen op de input van de professionals uit de tweede en derde lijn, waarbij het advies van de functionaris gegevensbescherming (FG) prevaleert boven de zienswijzen van anderen.

Gezamenlijk bewerkstelligen 1e, 2e en 3e lijn-verantwoordelijken dat binnen de gehele organisatie een volwassen AVG-organisatiecultuur bestaat, door middel van voorbeeldgedrag, aanspreekbaarheid, werkafspraken en het voorzien in de middelen waardoor iedereen laagdrempelig en gebruiksvriendelijk dit privacybeleid in de praktijk kan brengen. Het gaat om houding en gedrag. Iedereen binnen de organisatie, van portier tot de burgemeester, toont eigenaarschap.
We bespreken ervaringen met elkaar en staan open voor ideeën. Bij dilemma's gaan we de dialoog aan – óók met onze doelgroepen. Bijvoorbeeld via inspraakmogelijkheden, zoals burgerparticipatie, of met de Ondernemingsraad als het om medewerkers gaat.

4.2 Eigenaarschap in de tweede lijn

Om de kwaliteit en de voortgang van de privacybeleidsvoering te waarborgen, is er tweede lijn-ondersteuning. Die tweede lijn-ondersteuning wordt allereerst geboden door adviseurs op het gebied van privacy. Maar ook professionals op het gebied van informatiebeveiliging, informatiemanagement, informatiebeheer, communicatie, en ICT spelen een belangrijke rol als het gaat om de bescherming van persoonsgegevens.

Voor een gecoördineerde aanpak voeren de privacy officers (PO's) het Werkprogramma Privacy uit. Dit meerjarenplan is erop gericht om (a) AVG-kwaliteit te garanderen binnen alle gemeentelijke taakvelden en interne

bedrijfsvoering; en (b) die kwaliteit ook duurzaam te behouden bij veranderende omstandigheden. In dat kader werken de PO's volgens een jaarplan waarin prioriteiten zijn gesteld.

Het Werkprogramma Privacy wordt vastgesteld door het college, dat op deze manier aantoonbaar in control is. De directie stelt het jaarplan met de prioriteiten vast. De algemeen directeur draagt zorg voor het vrijmaken van de mensen en middelen die nodig zijn voor professionele en missiebewuste tweede-lijnondersteuning, zodat de uitvoering van dit privacybeleidskader realistisch en haalbaar is.

De opdracht aan de PO's is tweeërlei: (1) draag zorg voor algemene voorzieningen en schaalvoordelen op AVG-vlak; en (2) voorzie in zodanige ondersteuning van proceseigenaren dat zij hun verantwoordelijkheden kunnen némen – want ook voor hen dient privacybeleidsvoering een haalbare opdracht te zijn.
Dit laatste wil nadrukkelijk niet zeggen dat proceseigenaren privacybeleidsvoering aan PO's kunnen overlaten. Proceseigenaren zijn en blijven zelf verantwoordelijk. Maar daarvoor kunnen zij rekenen op tweede lijn-versterking.

4.3 Eigenaarschap in de derde lijn

Het eigenaarschap in de derde lijn betreft het toezicht op de interne naleving van privacywetgeving en het gemeentelijk beleid op dit vlak door de functionaris gegevensbescherming (FG). FG-toezicht is onafhankelijk van de eerste en tweede lijn.

Aan de hand van structurele en incidentele toetsing vormt de FG zich een beeld van het beschermingsniveau dat de gemeente daadwerkelijk biedt, conform de gestelde wettelijke criteria. In die zin is de FG naast onafhankelijk ook objectief.

Hij geeft op bestuursniveau gevraagd en ongevraagd advies, met name via zijn FG-verslag. Het FG-verslag is net zoals het accountantsverslag een vorm van rechtmatigheidscontrole, zij het dat de FG zich richt op de rechtmatigheid van verwerking van persoonsgegevens door of namens de gemeente.

De FG bewaakt of de gemeente de juiste koers vaart. In die zin verpersoonlijkt hij de borging van het privacybeleid en heeft hij een ombudsfunctie. Personen over wie de gemeente gegevens verwerkt of laat verwerken kunnen bij klachten daarover bij hem terecht. Denk hierbij aan klachten over de rechtmatigheid, juistheid of veiligheid van de gegevensverwerking.

De FG wordt door het gemeentebestuur naar behoren en tijdig betrokken bij alle aangelegenheden die verband houden met bescherming van persoonsgegevens. De gemeente ondersteunt hem in de uitvoering van zijn taken. Voor zover de FG besluit tot inspectie (FG-audit) heeft hij recht op toegang tot persoonsgegevens en verwerkingsactiviteiten, en documentatie hieromtrent.

Op de FG rust een geheimhoudingsplicht, in het bijzonder daar waar hij uit hoofde van zijn functie kennis neemt van persoonsgegevens. Dat betekent dat de FG ook voor het gemeentebestuur een vertrouwenspersoon / strategisch adviseur is.

Op schriftelijke stukken, zoals klachtbeoordelingen en het FG-verslag is de Wet open overheid van toepassing. Dit soort informatie wordt ook gedeeld in het kader van horizontaal toezicht volgens de Gemeentewet (raadscontrole) en met de accountant vanwege de financiële risico's die de gemeente loopt bij niet-naleving van privacywetgeving, met name de bepalingen in de AVG over individuele schadevergoeding en bestuurlijke boetes. Houd er daarom rekening mee dat FG-stukken ook gebruikt kunnen worden in gerechtelijke procedures of kunnen worden opgevraagd door de Autoriteit Persoonsgegevens (AP).

Het werk van de FG is gericht op het waarborgen van privacybeleidsvoering door de gemeente, zodat bestuurders met vertrouwen verantwoording kunnen afleggen.

RASCI	1e/4e lijn	Eigenaarschap
Responsible *Operationeel verantwoordelijk*	1	Directie / MT ('proceseigenaren', ook bij uitbesteding van taken aan aanbieders van informatiediensten en gemeenschappelijke regelingen)
Accountable *Bestuurlijk verantwoordelijk*	1	College, Raad, Burgemeester (de bestuursorganen)
Supportive *Ondersteunend*	2	Privacy Officers en andere professionals op o.a. het gebied van informatiebeveiliging (CISO/ISO), informatiebeheer, informatiemanagement, communicatie en ICT
Consulted *Raadgevend / toezicht*	3	FG
Informed *Geïnformeerd*	4	Inwoners Raad (t.b.v. horizontaal toezicht) Accountant Landelijk toezicht, met name de Autoriteit Persoonsgegevens

Gemeente Raalte

5. Behoorlijk bestuur met data

Hét uitgangspunt van privacybeleidsvoering is dat wij zorgdragen voor rechtmatige, behoorlijke en transparante verwerking van persoonsgegevens.

De gemeente verwerkt uitsluitend persoonsgegevens om te voorzien in een legitieme informatiebehoefte. Zonder die informatie gaat er iets fout in de gemeentelijke dienstverlening, taakuitoefening of bedrijfsvoering.
In de meeste gevallen is de doelgroep over wie de gemeente informatie verwerkt, hierbij gebaat. We zijn geen domme bureaucratie waar zich kafkaëske toestanden kunnen voordoen, maar gaan dat juist tegen (menselijke maat), die van geval tot geval verschillen. In die zin houden we net zozeer rekening met degenen die minder gemakkelijk onder één noemer kunnen worden geschaard.

De gemeente deelt om dezelfde redenen ook informatie met anderen waar dat nodig is, of ontvangt informatie van anderen. We zijn geen eiland maar maken deel uit van informatieketens. Het is belangrijk dat we ook hier de menselijke maat toepassen voor zover we daar invloed op hebben.

5.1 Op zoek naar de balans

Risico's voor personen bij verwerking van persoonsgegevens vragen altijd een afweging tussen belangen. Dat maakt het niet gemakkelijk om een duidelijke koers te varen en goede keuzes te maken. De privacywetgeving (met name de AVG) biedt echter een kader. Te beginnen met het volgende uitgangspunt:

> *De verwerking van persoonsgegevens moet ten dienste staan van de mens. Het recht op bescherming van persoonsgegevens heeft geen absolute gelding, maar moet worden beschouwd in relatie tot de functie ervan in de samenleving en moet conform het evenredigheidsbeginsel tegen andere grondrechten worden afgewogen.*

Andere grondrechten zijn bijvoorbeeld het recht op menselijke waardigheid, veiligheid, onderwijs en participatie. De verwerking van persoonsgegevens moet ten dienste staan van ons welzijn volgens de publieke waarden. Tegelijk prevaleert iemands individuele belang niet noodzakelijk, maar kunnen belangen van anderen zwaarder wegen – vooral als die andere belangen bij wet of gemeentelijke verordening zijn aangemerkt als van algemeen belang.

Het gaat om de balans. Daar waar de gemeente publiekrechtelijk of privaatrechtelijk een legitieme rol heeft en de uitvoering van deze rol gepaard gaat met verwerking van persoonsgegevens, is dat niet als zodanig een probleem. Risico's vloeien voort uit de kans dat we door het niet of gebrekkig verwerken van persoonsgegevens, sociale, psychische of financiële schade aanrichten, of misschien wel schade voor de gezondheid of gevaren voor de persoonlijke veiligheid.

5.2 Werkprogramma Privacy en jaarplannen

Via het Werkprogramma Privacy stellen wij prioriteiten en concrete doelen en maken wij de middelen beschikbaar om die doelen te bereiken. Aan de hand van ieders eigenaarschap en de Schaal van Erg houden we structureel vinger aan de pols. Ook DPIA's zijn instrumenteel, net zo goed als de lessen die wij trekken uit klachten en incidenten.

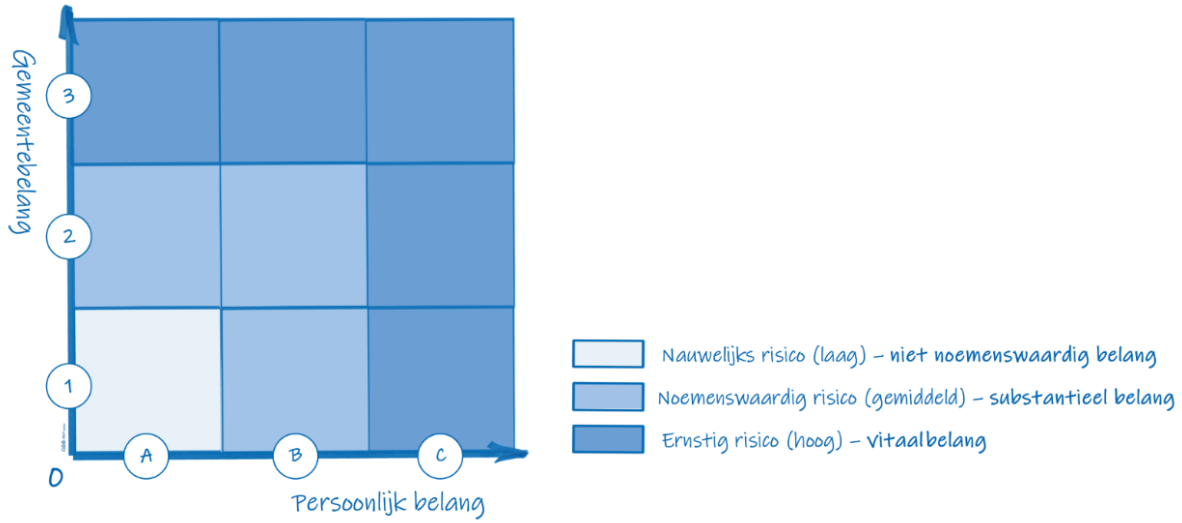
Het is aan de privacy officers om in het kader van het Werkprogramma Privacy, tijdig een jaarplan voor te stellen aan de directie om te voorzien in nieuwe oplossingen of bijstelling van bestaande oplossingen, inclusief realistische termijnen waarbinnen de doelen worden gerealiseerd en begroting van middelen.

- Door goedkeuring van het jaarplan geeft de directie aan de privacy officers opdracht tot uitvoering. Zij neemt hierin de aanbevelingen uit het jaarverslag van de FG mee.
- De privacy officers doen aan het einde van ieder kwartaal verslag aan de directie over het behalen van de gestelde doelen en eventuele knelpunten, met afschrift aan de FG.

5.3 De Schaal van Erg

We gebruiken de Schaal van Erg als methodiek voor objectieve risicoanalyse. Het is bedoeld om ons bewust te worden van de risico's en belangen die een gegevensverwerking met zich meebrengen, er de juiste prioriteit aan te geven en passende waarborgen te treffen zodat de risico's zich niet manifesteren.

We classificeren gemeentelijke activiteiten en bijbehorende informatieverwerking op deze schaal. We hanteren de Schaal van Erg ook bij de beoordeling van verzoeken, klachten en incidenten. Hoe hoger de risicoscore, hoe meer aandacht en prioritering nodig is, en hoe robuuster de maatregelen.



5.4 Data Protection Impact Assessments (DPIA)

Hét instrument om te kunnen voorzien in passende waarborgen is de Data Protection Impact Assessment (DPIA). Hiermee brengen we in kaart wat er mis kan gaan als informatiestromen *niet* met passende waarborgen zijn omkleed. Het is in essentie niet anders dan een soort milieueffectentoets. Maar dan gericht op de risico's voor de digitale leefomgeving.

DPIA's zijn geen invuloefening of een juridische toets, maar een logisch denkproces. Goede DPIA's worden gekenmerkt door dialoog met interne en eventueel externe stakeholders, in het bijzonder de doelgroep (meestal inwoners). Ons gaat het om inzicht in de kwetsbaarheden van een bepaalde aanpak en deugdelijke probleemanalyse:

1. Welke schade is voorzienbaar als we géén informatie verwerken (wat is de positieve impact van informatieverwerking)?
2. Welke schade is voorzienbaar als we gebrekkig informatie verwerken (wat is de negatieve impact van informatieverwerking)?
3. Welke bestuurlijke, organisatorische en technische maatregelen zijn vereist om te voorkomen dat er sprake kan zijn van gebrekkige informatieverwerking, gelet op de belangen bij deugdelijke informatieverwerking.

Door deze stappen te doorlopen begrijpen we waar welke oplossingen concreet nodig zijn voor een verantwoorde aanpak. Onze DPIA's maken dat inzichtelijk en leveren zinnige lijsten op van kritische kwaliteitseisen waarmee we integer recht doen aan de beginselen voor rechtmatige, behoorlijke en transparante verwerking van persoonsgegevens. Onze DPIA's leveren zo een praktisch handboek op waarmee wij grip creëren op onze werkwijze en samenwerking met anderen. DPIA's stellen ons in staat om de doeltreffendheid en doelmatigheid van privacybeleidsvoering in een specifieke context te bewaken. Tegelijk bieden ze ons de flexibiliteit om veranderingen door te voeren, door toetsing aan en - waar nodig – herijking van de DPIA.

Het behoort tot de managementtaken van proceseigenaren om DPIA's uit te voeren, door hiertoe opdracht te geven, zorg te dragen voor het voldoen aan de kwaliteitseisen uit de DPIA en hierover te rapporteren in de vorm van een verklaring aan het eindverantwoordelijke bestuursorgaan in hoeverre aan de kwaliteitseisen is voldaan. Het eventueel accepteren van restrisico's is ook een verantwoordelijkheid van de proceseigenaar. De kwaliteitseisen zijn voor ons Kritische Prestatie Indicatoren (KPI's).

De DPIA's zijn terug te vinden via een centraal overzicht van processen: het verwerkingsregister. De eigenaren in de eerste, tweede en derde lijn hebben zo inzicht in de privacy-aanpak en bereikte resultaten.

Voor zover maatregelen in de praktijk niet genoeg bescherming bieden, is het zaak om lering te trekken uit incidenten en klachten. De gemeente verbetert zichzelf op deze manier voortdurend. Het is aan de proceseigenaar om dat te bewerkstelligen en aan de algemeen directeur om hierop te sturen ('lerende organisatie').

6. Privacyrechten en incidentenmanagement

De AVG en Wpg voorzien in een aantal rechten voor personen over wie de gemeente informatie verwerkt. Voor dit soort verzoeken dienen duidelijke loketten te bestaan en moet zijn voorzien in een procedure voor de soepele afwikkeling ervan.

6.1 AVG/Wpg-verzoeken

Het doel van deze specifieke privacyrechten is in essentie mede-handhaving van de privacywetgeving door de personen in kwestie zelf ('empowerment'). Personen hebben als het ware recht op medebeheer, wat in ieder geval inhoudt dat zij recht hebben op inzage in gemeentelijke informatie die henzelf betreft. Bij fouten in de informatieverwerking, zowel inhoudelijk als beheersmatig, kunnen ook andere rechten van toepassing zijn (zoals het recht op verwijdering of rectificatie). De procedure voor soepele afwikkeling houdt in dat wij de verzoeken of klachten behandelen binnen de wettelijke termijnen.
Bij een AVG-verzoek of Wpg-verzoek is de proceseigenaar verantwoordelijk voor soepele afhandeling. Een privacy officer coördineert en bewaakt de juiste afhandeling.

6.2 fg@dowr.nl

De verzoeker / klager die zich niet kan vinden in de wijze waarop de gemeente op het verzoek is ingegaan, heeft het recht om hierover in contact te treden met de FG. De FG beoordeelt de klacht op kennelijke gegrondheid en kan in het kader daarvan nader onderzoek instellen.
De FG deelt zijn bevindingen met zowel de klager als de proceseigenaar. Als hij de klacht toewijst geeft hij daarbij concrete aanwijzingen hoe de situatie gerepareerd dient te worden. Naar gelang de ernst van de situatie kan hij ook besluiten om het verantwoordelijke bestuursorgaan en de portefeuillehouder te informeren dan wel aanwijzingen te geven. Mocht de klacht hem hebben bereikt met tussenkomst van de Autoriteit Persoonsgegevens (AP), dan bericht hij deze over zijn conclusies.

De FG wijst de verzoeker / klager op de mogelijkheid om eventueel een klacht in te dienen bij de AP of beroep in te stellen bij de rechter. Naar gelang de ernst van de situatie of de mate waarin de gemeente geen gevolg geeft aan zijn aanwijzingen, kan hij ook besluiten om bij de AP een hulpverzoek (handhavingsverzoek) in te dienen.

Personen kunnen ook over alle andere aangelegenheden die verband houden met de verwerking van hun gegevens contact opnemen met de FG.

6.3 Datalekken

De privacy officers dragen zorg voor een intern tweede lijn-loket voor het melden van (vermoedelijke) informatiebeveiligingsincidenten waarbij persoonsgegevens betrokken zijn (datalekken). De gemeente voert hiervoor een incidentenadministratie die wordt beheerd door de privacy officers.

Het gemeentebestuur voorziet in een plicht voor medewerkers en uitvoeringsorganisaties om incidenten zonder vertraging te melden bij het tweede lijn-loket. De privacy officers zetten de acties uit die nodig zijn naar gelang het karakter van het incident en de risicoclassificatie. In geval van een substantieel of hoog risico wordt er melding gedaan aan de AP en worden gedupeerden geïnformeerd. De betreffende proceseigenaar is verantwoordelijk voor de afhandeling van het datalek.

Het gemeentebestuur en de directie waarborgen *just culture*, dat wil zeggen een organisatiecultuur waarin je veilig incidenten kunt melden, ook al ben je zelf de veroorzaker.

7. Handhavingsbeleid

Dit privacybeleidskader is van strategisch belang en niet vrijblijvend. We handhaven de privacybeleidsvoering daarom via het eigenaarschap zoals beschreven in hoofdstuk 4 van dit document. We verwachten dat iedereen zijn/haar verantwoordelijkheid néémt volgens de rol die je hebt binnen het RASCI-model. Werken op het kwaliteitsniveau van de AVG en Wpg impliceert dat we beschikken over een volwassen organisatiecultuur.

7.1 Handhaving in de eerste en tweede lijn

De privacy-aanpak waarborgt dat we het goede doen, en het goede *goed* doen. Dit op een zodanige manier dat we het steeds kunnen uitleggen en onze doelgroepen het begrijpen. Transparantie (communicatie) is daarmee evenzeer onderdeel van ons handhavingsbeleid. Dat zijn geen lege woorden maar zijn gestoeld op SMART-geformuleerde afspraken, die integraal onderdeel zijn van onze managementcyclus.

1. Via de interne verantwoording stuurt de algemeen directeur op de nakoming van afspraken door de proceseigenaren.
2. Via de DPIA-aanpak sturen de proceseigenaren op hun beurt op het bestaan en de goede werking van passende waarborgen – die steeds een mix zijn van organisatorische en technische maatregelen ('hard en soft controls').
3. Bij uitbesteding van taken en/of gegevensverwerking aan uitvoeringsorganisaties bewaken proceseigenaren (eventueel in samenwerking met contractmanagers) aan de hand van service level-afspraken dat de uitvoerende partij(en) minimaal dezelfde garanties bieden als wat de gemeente volgens de DPIA voor het desbetreffende taakgebied zelf nodig heeft.
4. Bij participatie met meerdere instanties in een collectieve oplossing zoals een BV of samenwerkingsverband volgens de Wet gemeenschappelijke regelingen, geldt hetzelfde als bij uitbesteding maar waarborgt het betreffende bestuursorgaan bovendien ook via de participatieregeling goed (mede-)eigenaarschap. Personen over wie informatie wordt verwerkt kunnen zo bij klachten of incidenten zonder meer op de gemeente terugvallen.

Zo bieden we informationele rechtsbescherming in het digitale tijdperk, eerlijke belastingheffing, de juiste hulp, publieke veiligheid, publieke gezondheid, maar ook veilige en gezonde werkomstandigheden.

Voor management van het Werkprogramma Privacy, het documenteren van DPIA's, het bijhouden van het verwerkingsregister en monitoring op de nakoming van afspraken hanteren wij een privacy managementsysteem, omdat we vanwege de complexiteit anders het overzicht verliezen. Eerste, tweede en derde lijn-eigenaren krijgen aan de hand hiervan ondersteuning en beschikken over dashboards voor de bewaking van nakoming van afspraken.

7.2 Handhaving in de derde lijn

De FG beoordeelt of de handelingen van het gemeentebestuur en het privacymanagement in lijn zijn met de ambities, doelstellingen en afspraken volgens dit borgingsdocument. Hij doet dit op basis van incidentele en structurele toetsing.

- Incidentele toetsing zijn de inspecties/audits waartoe hij ad hoc besluit, wat met name het geval kan zijn naar aanleiding van incidenten en klachten.
- Structurele toetsing is het permanente toezicht dat de FG uitoefent in de vorm van dagelijkse ervaringen en de jaarlijkse FG-audits.

Op basis hiervan geeft hij een beoordeling af in de vorm van een jaarlijks verslag aan het gemeentebestuur (FG-verslag). Hij kan ook besluiten tot tussentijdse beoordelingen of het afgeven van aanwijzingen. Mocht daar door de gemeente onvoldoende mee worden gedaan, kan hij de AP zo nodig verzoeken om te interveniëren.

7.3 Handhaving in de vierde lijn

De handhaving in de vierde lijn betreft de correctiemechanismes die in werking horen te treden naar aanleiding van de beoordelingen door het FG-toezicht. Als uit het FG-verslag zou blijken dat de gemeente onvoldoende stuurt op privacy-zaken, is dat:

- Voor de accountant reden om te waarschuwen tegen de financiële risico's van individuele schadeclaims en bestuurlijke boetes;
- Voor de gemeenteraad reden om in het kader van haar controlerende taken volgens de Gemeentewet, het college van B&W of de burgemeester verantwoording te laten afleggen;
- Voor de AP informatie die interventie vanuit het landelijk toezicht kan rechtvaardigen.

Gemeente Raalte

8. Beleidsevaluatie

8.1 Periodiek onderzoek naar doelmatigheid en doeltreffendheid

Overeenkomstig artikel 24 AVG en artikel 4a Wpg onderzoekt het college 5-jaarlijks de doelmatigheid en doeltreffendheid van de privacybeleidsvoering. Leidend in dit onderzoek zijn de FG-beoordelingen van de beleidsvoering over dit tijdvak en zijn adviezen aan het gemeentebestuur, zoals deze met name blijken uit zijn jaarverslagen. Deze zijn de graadmeter voor de mate waarin de gemeente erin slaagt om bescherming te bieden op het kwaliteitsniveau van de privacywetgeving en dat niveau structureel vast te houden.

- Voor zover uit de FG-verslagen blijkt dat de gemeente op of boven het kwaliteitsniveau opereert, inventariseert het college de succesfactoren en wellicht aspecten voor verdere optimalisatie, in samenspraak met overige eigenaren in de eerste en tweede lijn. De doelmatigheid en de doeltreffendheid van de privacy-aanpak als zodanig, staat afdoende vast. Het college analyseert of de aanpak ook gedurende het komende tijdvak houdbaar is, gelet op bestuurlijke, organisatorische, technologische, maatschappelijke en wettelijke veranderingen. De vooruitblik wordt verdisconteerd in het werkprogramma voor de nieuwe periode zodat de gemeente zich niet laat overrompelen maar veerkrachtig inspeelt op de veranderende omstandigheden.

- Voor zover uit de FG-verslagen blijkt dat de gemeente onder het kwaliteitsniveau opereert, onderzoekt het college de bestuurlijke en organisatorische faalfactoren. Vast staat dat de werking van de privacy-aanpak op het moment van evaluatie nog ondoelmatig en ondoeltreffend is. De vraag is wat de gemeente ervan weerhoudt om op het juiste niveau te opereren en welke bestuurlijke en organisatorische reparaties vereist zijn om in de komende periode alsnog dit kwaliteitsniveau te bereiken. Voor zuivere reflectie is het zaak om dit onderzoek te laten uitvoeren door een onafhankelijk bureau dat gespecialiseerd is in verandermanagement in de publieke sector. De reparatiepunten hebben prioriteit in het werkprogramma voor de nieuwe periode, ook rekening houdend met te verwachten bestuurlijke, organisatorische, technologische, maatschappelijke en wettelijke veranderingen.

8.2 Onderzoek bij ontbreken van FG-verslagen

In het geval dat de gemeente niet beschikt over FG-verslagen waarin beoordeling plaatsvindt van de gemeentelijke privacybeleidsvoering en advisering op bestuursniveau, behelst het onderzoek in eerste plaats de vraag of:

1. De gemeente beschikt over een FG die voldoet aan de wettelijke eisen; en zo ja
2. Hem naar behoren de ruimte wordt geboden voor professionele uitvoering van taken.

De noodzaak voor het stellen van deze vragen kan ook blijken uit rekenkameronderzoek of onderzoek door de auditcommissie. Het kernprobleem is dat het wettelijk toezicht vanuit de derde lijn kennelijk niet functioneert. Dat betekent in principe dat de privacybeleidsvoering onvoldoende met waarborgen is omkleed en in strijd is met de wet. Daarmee is de aanpak ook niet doelmatig en doeltreffend.
Onderzoek naar de FG-functie wordt uitgevoerd door een onafhankelijk bureau met bewezen expertise op het vlak van FG-beroepsbeoefening (peer-review).