PRIVACY BELEIDSKADER

Datum: 4 juni 2019

Versie: 1.1

Inhoudsopgave Privacy beleidskader

1. Kernpunten

1.1. Inleiding

Binnen de gemeente Venlo wordt gewerkt met een aanzienlijk aantal persoonsgegevens[1] van burgers, medewerkers en (keten)partners. Er worden veel persoonsgegevens verzameld voor het goed uitvoeren van gemeentelijke taken en om te voldoen aan wettelijke verplichtingen. Daarnaast gebruikt de gemeente persoonsgegevens voor bijvoorbeeld haar salarisadministratie en om statistisch onderzoek te kunnen doen zodat zij haar beleid kan verbeteren. Alle betrokkenen moeten er op kunnen vertrouwen dat de gemeente zorgvuldig en veilig met deze persoonsgegevens omgaat.

Nieuwe technologische ontwikkelingen, innovatieve voorzieningen, globalisering en een steeds meer digitale overheid stellen andere eisen aan de bescherming van gegevens en privacy. De gemeente Venlo is zich hiervan bewust en zorgt dat privacy, door middel van een continu verbeterproces, gewaarborgd wordt, onder andere door maatregelen op het gebied van informatiebeveiliging, dataminimalisatie, transparantie en gebruikerscontrole.

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

1.2. Voor wie?

Het privacybeleidskader gemeente Venlo bevat afspraken tussen de bestuursorganen van de gemeente Venlo (bestaande uit het college van burgemeester en wethouders (hierna: “het college”), de gemeenteraad (hierna: “de raad”) en de burgemeester (hierna gezamenlijk te noemen: “de bestuursorganen”)) enerzijds en het management anderzijds en vormt daarnaast een kader waarbinnen medewerkers die persoonsgegevens verwerken[2] dienen te opereren.

1.3. Doel

Met de vaststelling van dit privacybeleidskader willen de bestuursorganen drie doelen bereiken:

1) De visie van de gemeente Venlo op het onderwerp privacy vastleggen;

2) Verantwoordelijkheden in dit kader beleggen;

[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.

3) Kaders stellen om te borgen dat de gemeente Venlo op een behoorlijke en zorgvuldige wijze persoonsgegevens verwerkt in overeenstemming met de wet.

1.4. Visie

De gemeente Venlo ziet bescherming van persoonsgegevens als een zaak van behoorlijk bestuur. Inwoners en medewerkers moeten erop kunnen vertrouwen dat persoonsgegevens rechtmatig, zorgvuldig en veilig worden verwerkt. De bestuursorganen zorgen daarom voor de randvoorwaarden van een privacybewuste organisatiecultuur en voeren in dat kader een adequaat privacybeleid. Zij zijn transparant over hun gegevensverwerkingen en de manier waarop deze gegevens worden beschermd. Zij zorgen voor een goede balans tussen adequate bescherming van privacy en effectieve processen om betrokkenen te bedienen.

Met behulp van dit privacybeleidskader wil de gemeente richting maatschappij en betrokkenen kunnen verantwoorden en aantonen dat persoonsgegevens bij haar in goede handen zijn.

1.5. Reikwijdte

Dit privacy beleidskader is van toepassing op:

- de gehele organisatie;
- alle processen waarbinnen persoonsgegevens worden verwerkt, waaronder processen die de gemeente Venlo uitbesteedt, inkoopt of op een andere manier organiseert;
- alle mogelijke groepen betrokkenen waarvan de gemeente persoonsgegevens verwerkt, dus onder meer op burgers en medewerkers;
- informatiesystemen waarin persoonsgegevens worden verwerkt, waarvoor de gemeente (intern en extern) verantwoordelijk is;
- alle ruimten en middelen die door gemeenteambtenaren intern en extern worden gebruikt bij de uitoefening van hun taak waar(op) persoonsgegevens worden verwerkt;
- alle onderdelen, objecten en gegevensverzamelingen van de gemeente waarin de verwerking van persoonsgegevens een rol speelt;
- de hele verwerkingscyclus van persoonsgegevens, van het ontvangen, verzamelen en genereren, het dagelijks gebruik en de opslag/archivering tot en met de vernietiging daarvan;
- verwerkingen via alle soorten gegevensdragers, zowel digitaal als op papier.

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. Informatieveiligheid is een randvoorwaarde voor eerbiediging van de persoonlijke levenssfeer bij de verwerking van persoonsgegevens. In het informatiebeveiligingsbeleid van de gemeente Venlo zijn uitgangspunten beschreven om de beschikbaarheid, integriteit en vertrouwelijkheid van gemeentelijke informatievoorzieningen en persoonsgegevens te waarborgen.

Archiefbeleid, managementinformatie, gegevensvernietiging
De verantwoordelijkheid voor de archivering binnen de gemeente Venlo is vastgelegd in de Archiefverordening en het Besluit informatiebeheer Gemeente Venlo. Deze voorschriften zijn gebaseerd op de Archiefwet. Hierin zijn tevens bepalingen opgenomen over vernietiging van gegevens en documenten. Privacywetgeving en – beleid en de Archiefwet en – beleid moeten in onderlinge samenhang bekeken worden. Bij de overbrenging conform de Archiefwet van gegevens en bescheiden naar de gemeentelijke archiefbewaarplaats dienen de privacywet- en regelgeving in acht te worden genomen.

Integriteit
Privacybewust werken en integer zijn raken elkaar. Integer zijn is niet voldoende om te voldoen aan privacywetgeving, 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 op grond van de Ambtenarenwet.

2. Privacymanagement

In dit hoofdstuk wordt de wijze waarop privacymanagement is ingericht met de bijbehorende rollen en verantwoordelijkheden beschreven.

2.1. Context

Privacy is niet het domein van automatisering, hoewel de problematiek van databescherming vooral 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 maken van afspraken met partijen met wie informatie wordt gedeeld en om voorlichting aan betrokkenen. De gehele organisatie is betrokken bij de verwerking van persoonsgegevens en dus is het logisch dat privacy wordt belegd waar alle lijnen samenkomen: het college[3], dat in veel gevallen de verantwoordelijke voor een verwerking is.

Privacy dient geborgd te worden middels een vaste plek binnen het verantwoordelijke bestuursorgaan/ management, met een vaste portefeuillehouder[4] die de tijd, kennis en bestuurskracht heeft om in te grijpen in alle onderdelen van de organisatie en haar processen waarin persoonsgegevens verwerkt worden. Een goed privacymanagement vergt goede werkwijzen, geboden en verboden. Het vergt overzicht over de totale keten waarbinnen data van de organisatie rond gaan en het maken van afspraken waarbinnen dit gebeurt. De verwerking van persoonsgegevens moet worden gemonitord en er moet worden ingegrepen als contractpartners aan wie de verwerking is uitbesteed hun afspraken niet nakomen. Goed privacymanagement 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.

[3] Dit ziet op de verwerkingen waarvoor het college verantwoordelijk is. Voor de verwerkingen waarvoor de raad en de burgemeester verantwoordelijk zijn geldt dit niet. Zie daarvoor noot 7.
[4] Voor zover het de verwerkingen betreft waarvoor het college verantwoordelijk is.

Om daadwerkelijk te kunnen waarborgen dat privacybescherming ingebed wordt in de gemeentelijke organisatie is het noodzakelijk dat alle medewerkers die persoonsgegevens gebruiken dit op een zorgvuldige wijze doen en het proces beheerst wordt vanuit een centrale visie. Daarvoor is onderstaand governance model ingericht.

2.2. Verantwoordelijkheid voor naleving van privacywet- en regelgeving en privacybeleid

De bestuursorganen van de gemeente Venlo zijn verantwoordelijk voor de naleving van privacywet- en regelgeving 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 verwerkingsverantwoordelijke[5] in de zin van de AVG. De bestuursorganen bevorderen de beschikbaarheid van voldoende middelen om privacybescherming passend te waarborgen.

Het college en de burgemeester leggen verantwoording af aan de raad over de status van de uitvoering van het privacybeleid en zullen binnen de jaarlijkse planning & control cyclus de gemeenteraad informeren over de risico's en over de getroffen beheersmaatregelen op het gebied van privacy. Het college en de burgemeester melden bijzonderheden ten aanzien van gegevensverwerkingen, te denken valt bijvoorbeeld aan ernstige datalekken, proactief aan de gemeenteraad.

2.3. Rollen en verantwoordelijkheden binnen de gemeentelijke organisatie

Een belangrijk uitgangspunt in privacywetgeving is accountability: de verwerkingsverantwoordelijke is verantwoordelijk voor de naleving van de in privacywetgeving neergelegde eisen en kan aantonen dat hij hieraan voldoet[6] (verantwoordingsplicht). Om hieraan te kunnen voldoen dient binnen de gemeentelijke organisatie sturing en monitoring plaats te vinden op naleving van privacywet- en regelgeving en privacybeleid. Hiertoe zijn de volgende rollen en verantwoordelijkheden belegd.

Raad

Het college legt jaarlijks verantwoording af aan de raad over de status van de uitvoering van het privacybeleid, onder meer over de risico's en beheersmaatregelen.

Portefeuillehouder privacy[7]

Het college wijst uit haar midden een portefeuillehouder privacy aan. Het college handhaaft haar

[5] Zie artikel 4 sub 7 AVG. Verwerkingsverantwoordelijke: 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.
[6] Zie artikel 5 lid 2 AVG.
[7] Voor de verwerkingen die onder verantwoordelijkheid van de raad plaatsvinden vervult de raadsgriffier zowel de rollen van portefeuillehouder privacy, directie als teamleider. Voor verwerkingen die onder verantwoordelijkheid van de burgemeester plaatsvinden vervult de kabinetschef de rollen van portefeuillehouder privacy, directie en teamleider.

privacybeleid op basis van afspraken over interne rekenschap zoals de planning en controlcyclus. Het college neemt bij ontwikkeling van beleid privacywet- en regelgeving en het privacybeleid in acht.

De portefeuillehouder privacy ziet toe op de ontwikkeling en uitvoering van thematisch privacy beleid (denk bijvoorbeeld aan specifek beleid voor HR of de uitvoering van de Jeugdwet) door teamleiders/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.

Het directieteam

Het college belegt de nadere invulling van privacymanagement bij het directieteam. Het directieteam wijst een van haar leden aan als portefeuillehouder op directieniveau. Het directieteam is verantwoordelijk voor de integrale sturing van de ambtelijke organisatie op naleving van privacywet- en regelgeving en privacybeleid. Zij legt verantwoording af aan het college over het gevoerde privacybeleid via de portefeuillehouder privacy. In ieder verantwoordingsgesprek van de directeur met een teamleider is privacy gespreksonderwerp.

Teamleiders/proceseigenaren

Voor ieder primair of ondersteunend proces binnen gemeente Venlo is een teamleider/proceseigenaar aangewezen die zorgdraagt voor de vormgeving, uitvoering en monitoring van privacybeheersmaatregelen binnen zijn team en verwerkingsproces en die aanspreekbaar is op het effectief waarborgen van privacy in dat proces.

Zie voor een nadere toelichting van de rol van teamleider/proceseigenaar paragraaf 2.4.

Interne toezichthouder

De bestuursorganen hebben een Functionaris voor de Gegevensbescherming (FG) aangesteld als interne toezichthouder op de naleving van privacybeleid en privacywet- en regelgeving en als adviseur voor het management inzake privacyvraagstukken.

Zie voor een nadere toelichting van de rol van Functionaris voor de Gegevensbescherming paragraaf 2.5.

Privacy officer

De Privacy officer ondersteunt en adviseert het management en de medewerkers van de gemeente Venlo bij de praktische invulling van het privacybeleid en privacywet- en regelgeving. Hij/ zij ondersteunt ook de FG bij zijn taken. De Privacy officer wordt functioneel en hiërarchisch aangestuurd door de teamleider Juridische Zaken.

Zie voor een nadere toelichting van de rol van Privacy Officer paragraaf 2.6.

Informatiebeveiligingsfunctionaris

De FG stemt regelmatig af met de Chief Information Security Officer (CISO) over de raakpunten van informatieveiligheid en privacy binnen de gemeentelijke processen.

Medewerkers

Alle medewerkers[8] (inclusief inhuur en externen) van de gemeente Venlo zijn ervoor verantwoordelijk dat zij bij de uitoefening van hun werkzaamheden conform het privacybeleid en op basis van de daarin beschreven kernprincipes en uitgangspunten (zie paragraaf 3.2) werken. Zij dienen zich hiervan bewust te zijn en te voldoen aan hun geheimhoudingsverplichting. Zij hebben zo een belangrijke bijdrage aan de rechtmatige, behoorlijke en transparante verwerking van persoonsgegevens binnen de gemeente.

2.4. Teamleider/proceseigenaar

Voor ieder primair of ondersteunend proces binnen gemeente Venlo is een teamleider/proceseigenaar aangewezen die zorgdraagt voor de vormgeving, uitvoering en monitoring van privacybeheersmaatregelen binnen zijn team en verwerkingsproces en die aanspreekbaar is op het effectief waarborgen van privacy in dat proces. In procesbeschrijvingen wordt beschreven op welke wijze hij daaraan invulling dient te geven.

De teamleider/proceseigenaar rapporteert over wat hij doet en wat de kwaliteit is van de uitvoering van het beleid aan directie/portefeuillehouder.

Teamleiders/proceseigenaren dienen de FG – gevraagd en ongevraagd – op de hoogte te brengen van relevante ontwikkelingen/ informatie voor wat betreft de realisatie van passende privacy-waarborgen binnen hun processen.

Teamleiders/proceseigenaren nemen privacy als structureel onderdeel op in hun werkoverleggen. De organisatie werkt zo actief aan privacybewustzijn, het opbouwen van kennis bij medewerkers en aan een verantwoorde procesuitvoering.

2.5. Functionaris voor de Gegevensbescherming (FG)

Voor onafhankelijk toezicht op de naleving van privacywet- en regelgeving en het privacybeleid hebben de bestuursorganen een FG aangesteld. De FG heeft een onafhankelijke positie in de organisatie. De werkzaamheden die de FG uitvoert hebben een wettelijke grondslag.

De taken van deze functionaris zijn, kort samengevat, informeren, adviseren, toezicht houden, bewustwording creëren, en optreden als contactpersoon van de Autoriteit Persoonsgegevens.

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

Per post:
Gemeente Venlo
T.a.v. de Functionaris Gegevensbescherming

[8] Voor de raad zijn dit de raadsadviseurs.

Postbus 3434
5902 RK Venlo

Per e-mail: fg@venlo.nl

De FG ziet er samen met de verantwoordelijke portefeuillehouder en in samenspraak met de concerncontroller op toe dat er een privacy monitorings- en verantwoordingsplan wordt opgesteld en dat dit wordt uitgevoerd, en voert daarnaast zelfstandig controles uit. De FG ziet toe op implementatie van maatregelen en naleving daarvan door de gemeentelijke organisatie.

De FG treedt op als adviseur voor de directie, het college, de raad en burgemeester op beleidsniveau. De FG heeft 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) hebben de bestuursorganen een Statuut vastgesteld waarin positie, taken en bevoegdheden van de FG vastgelegd zijn.

2.6. Privacy officer

De privacy officer ondersteunt enerzijds de gemeentelijke organisatie bij de praktische invulling van de gestelde privacykaders en ondersteunt anderzijds de FG in de uitoefening van zijn taken. De privacy officer heeft de volgende hoofdtaken:

- Adviseren over het beleid/ de visie van de gemeente Venlo op het gebied van privacy;
- Adviseren in het kader van ad-hoc informatievragen over privacy, het verhogen van het privacy-bewustzijn binnen de organisatie en een bijdrage leveren aan de opstelling van privacy-protocollen en overeenkomsten in de gehele organisatie;
- Volgen van actualiteiten, wet- en regelgeving en jurisprudentie omtrent privacy;
- Structurele contacten onderhouden met de privacy officers van ketenpartners en regiogemeenten;
- Adviseren over de inrichting en veiligheid van gegevensverwerkingen en de daarbij behorende datasystemen;
- Ondersteuning van teamleiders/proceseigenaren bij de vervulling van de actieve informatieplicht richting betrokkenen en in de algehele communicatie rondom privacy;
- Het bewaken en borgen van de rechten van betrokkenen en de uitvoering van procedures die hiermee verband houden door teamleiders/proceseigenaren;
- Advisering en ondersteuning in geval van beveiligingsincidenten/ datalekken conform de vastgestelde procedure meldplicht datalekken;
- Het leveren van een bijdrage aan toezicht en sturing op de naleving van het privacybeleid en privacywet- en regelgeving;

· Oog hebben voor maatschappelijke ontwikkelingen en in staat zijn een brug te bouwen tussen maatschappelijke ontwikkelingen en privacy-waarborgen.

3. Privacy beleidskader Gemeente Venlo

3.1. Algemeen

De bestuursorganen zijn verantwoordelijk voor het opstellen, uitvoeren en handhaven van een privacy beleidskader.

Hiervoor gelden onder andere de volgende wettelijke kaders:

- de Algemene Verordening Gegevensbescherming (AVG);
- de Uitvoeringswet Algemene Verordening Gegevensbescherming.

3.2. Taakstelling en uitgangspunten

De gemeente Venlo gaat op een zorgvuldige manier met persoonsgegevens om en respecteert de privacy van betrokkenen. Gelet op de visie, verwoord in paragraaf 1.4, hecht de organisatie aan een goede balans tussen adequate bescherming van privacy en praktische werkprocessen. 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. Denk bijvoorbeeld aan het verwerkingsregister, de privacyverklaring op de website van de gemeente en informatie die voor aanvang van een verwerking aan een betrokkene wordt verstrekt. In uitzonderingsgevallen kunnen de bestuursorganen 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
De gemeente verwerkt alleen de persoonsgegevens die minimaal noodzakelijk zijn voor het vooraf bepaalde doel.

Bewaartermijn
Het bewaren van persoonsgegevens kan nodig zijn om de gemeentelijke taken goed uit te kunnen oefenen of om wettelijke verplichtingen te kunnen naleven. Persoonsgegevens mogen echter niet langer worden bewaard dan noodzakelijk is voor het doel waarvoor ze nodig zijn. De toepasselijke

bewaartermijnen worden beschreven in verschillende wetten. Daar waar er geen wettelijke bepaling is die voorziet in een verplichte bewaartermijn, dient het college een eigen besluit over de bewaartermijn te nemen. Zoals toegelicht onder 1.6 zal aan de hand van de Archiefwet en het archiefbeleid van de gemeente Venlo, in samenhang met privacywetgeving en – beleid, bekeken moeten worden hoe lang persoonsgegevens in een concreet geval bewaard mogen worden. De privacy officer en de gemeente archivaris adviseren in voorkomende gevallen.

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 privacybeleid 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. Deze dienen te worden afgestemd op het risico en de gevoeligheid van de binnen een proces en informatiesysteem verwerkte gegevens. Om dit mogelijk te maken dienen alle processen en informatiesystemen die gegevens verwerken een eigen dataclassificatie te hebben. Dataclassificatie heeft als doel om de beschikbaarheid, integriteit en vertrouwelijkheid van het proces en het informatiesysteem passend bij het risiconiveau te bepalen, zodat beheersmaatregelen daarop kunnen worden afgestemd. De binnen de gemeente Venlo gehanteerde methodiek, de daarbij geldende beleidsuitgangspunten en verantwoordelijkheden om data te classificeren zijn vastgelegd in separaat beleid.

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 andere wettelijke grondslag.

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 er onder meer voor 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 betrokkene 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. Teamleiders/proceseigenaren dragen er zorg voor dat hun processen conform het subsidiariteitsbeginsel ingericht zijn. De privacy officer staat hen hierin met advies terzijde.

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 is voor het uitoefenen van de taak. Teamleiders /proceseigenaren dragen er zorg voor dat hun processen conform het proportionaliteitsbeginsel ingericht zijn. De privacy officer staat hen hierin met advies terzijde.

Privacy by design
Bij de ontwikkeling van producten en diensten is er aandacht voor privacy en wordt gebruik gemaakt van privacy-verhogende maatregelen (ook wel *privacy enhancing technologies* of PET genoemd). Teamleiders/proceseigenaren dragen er zorg voor dat hun processen conform het principe privacy by design ingericht zijn. De privacy officer staat hen hierin met advies terzijde.

Privacy by default
Het concept van privacy by default verplicht organisaties om instellingen en functies van producten of diensten standaard (by default) op de meest privacy vriendelijke stand te zetten. Teamleiders /proceseigenaren dragen er zorg voor dat hun processen conform het principe privacy by default ingericht zijn. De privacy officer staat hen hierin met advies terzijde.

3.3. Kapstokregeling

Het privacybeleidskader schept een algemeen kader voor de omgang met persoonsgegevens. In paragraaf 3.1 is reeds aangegeven 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. De gemeente dient zich ook aan die aanvullende privacyregels te houden.

Teamleiders/proceseigenaren geven, waar nodig, via separaat uitvoeringsbeleid (denk bijvoorbeeld aan specifek beleid voor HR of de uitvoering van de Jeugdwet) nadere invulling aan het privacybeleidskader, in samenspraak met de privacy officer. Dat beleid zal door de bestuursorganen worden vastgesteld.

4. Inbedding binnen de organisatie

4.1. Register van verwerkingen (artikel 30 AVG)

De bestuursorganen zijn verantwoordelijk voor het aanleggen van een register van alle verwerkingen waarvan zij de verwerkingsverantwoordelijke zijn. Het register beschrijft alle verwerkingen van persoonsgegevens binnen de gemeentelijke organisatie.

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;
- indien mogelijk, een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen.

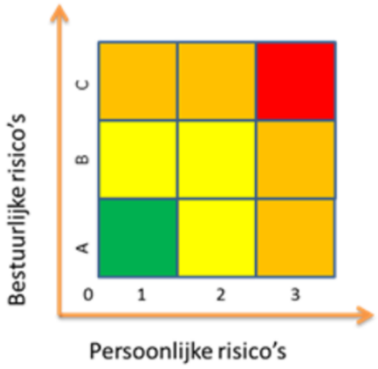
Teamleiders/proceseigenaren zijn verantwoordelijk voor het melden van nieuwe verwerkingen en relevante wijzigingen in bestaande verwerkingen, waarna deze in het register verwerkt worden. Voor het beheer van bestaande verwerkingen en registratie van nieuwe verwerkingen zal de gemeente een interne procedure hanteren.

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 continu proces van veranderen en verbeteren. Privacymanagement 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 data protection impact assessments (hierna: DPIA's, zie artikel 35 AVG). Met een DPIA worden de effecten en risico's van nieuwe of bestaande verwerkingen beoordeeld op de bescherming van privacy. Teamleiders/proceseigenaren zijn er voor verantwoordelijk dat DPIA's worden uitgevoerd indien in hun verwerkingsproces sprake is van een hoog risico voor de privacyrechten van betrokkenen. Voor de beoordeling of er een DPIA plaats moet vinden dient een teamleider/proceseigenaar een privacy baseline toets (die onderdeel is van de bredere baseline toets) in te vullen of advies te vragen aan de privacy officer. In overleg met de privacy officer zal vervolgens een DPIA in gang gezet worden.

De effecten van een verwerking, zowel profijt als risico's voor personen en de gemeente, worden door middel van een DPIA 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 persoonlijke- en bestuurlijke risico's in kaart gebracht. Deze vormt het vertrekpunt voor het maken van beleidskeuzes.



De kwaliteit van de omgang met privacyvraagstukken wordt verhoogd door op verschillende niveaus en vanuit verschillende rollen telkens weer de PDCA-cyclus[9] te doorlopen. Hierdoor ontstaat een evenwichtig privacy- beheersingssysteem.

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

4.3. Meldplicht datalekken

Waar gehakt wordt vallen spaanders. Datalekken zijn helaas niet in alle gevallen te voorkomen.

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 Venlo als overheidsorgaan hierin heeft, is zij op grond van wetgeving verplicht een datalek zonder onredelijke vertraging, maar uiterlijk binnen 72 uur, 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[10] ook onverwijld aan betrokkenen worden gedaan.

Om aan de wet te kunnen voldoen hanteren de bestuursorganen een vastgestelde interne procedure, genaamd de procedure meldplicht datalekken, die hierop aansluit. Onderdeel van deze procedure vormt evaluatie van geconstateerde datalekken om incidenten in de toekomst waar mogelijk te voorkomen, dan wel het risico daarop/ de gevolgen daarvan te verkleinen. Met externe partijen en opdrachtnemers die samen met of in opdracht van de gemeente persoonsgegevens verwerken zijn afspraken gemaakt hoe te handelen in geval van een datalek. Het melden van een (vermoedelijk) datalek door betrokkenen is mogelijk via het e-mailadres dat vermeld staat op de website van de gemeente Venlo.

De Autoriteit Persoonsgegevens is bevoegd om (het niet (tijdig) melden van) 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 met externe partners en waarbij een verwerking van persoonsgegevens plaatsvindt, worden convenanten, verwerkersovereenkomsten en geheimhoudingsverklaringen aangegaan. Teamleiders/proceseigenaren dienen zorg te dragen voor het maken van deze afspraken en er voor te zorgen dat deze afspraken bevoegd worden vastgelegd. 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 teamleiders/proceseigenaren hierin.

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

[10] Artikel 33 AVG

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

4.5. 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 privacywet- en regelgeving en privacybeleid worden nageleefd. Het is van groot belang dat medewerkers die werken met persoonsgegevens weten wat er van hen verwacht wordt en hoe zij zorgvuldig om dienen te gaan met persoonsgegevens. Zij dienen over voldoende privacykennis te beschikken om in staat te zijn te beoordelen welke gegevens nodig zijn voor het uitvoeren van werkprocessen en in lijn met het privacybeleid te kunnen handelen.

Beleid en maatregelen alleen zijn niet voldoende om risico's op het gebied van de verwerking van persoonsgegevens uit te sluiten. Privacybewustzijn wordt daarom binnen de gemeente Venlo 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 moet een constante afweging worden gemaakt tussen "need to know" en "nice to know", waarbij voor wat betreft de laatste categorie geen persoonsgegevens worden verwerkt.

Teamleiders/proceseigenaren zorgen er voor dat informatie over gegevensbescherming herhaaldelijk onder de aandacht wordt gebracht van medewerkers. Zij worden hierin bijgestaan door de FG en privacy officer. Medewerkers worden getraind in privacy-bewust handelen door middel van presentaties, workshops en trainingen en het altijd voorhanden hebben van een aanspreekpunt. Hiertoe wordt een privacy communicatieplan opgesteld.

5. Privacyservices

5.1. Rechten van betrokkenen

Om betrokkenen in staat te stellen controle uit te oefenen over hun eigen persoonsgegevens zijn in wetgeving diverse rechten neergelegd. De gemeente hecht eraan dat de procedures die waarborgen dat betrokkenen op effectieve wijze hun rechten uit kunnen oefenen op transparante wijze ingericht zijn. Hierbij wordt gebruik gemaakt van het navolgende kader:

Wet openbaarheid van bestuur

Via de Wet openbaarheid van bestuur (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 gegevens aan de gemeente ter beschikking stellen, worden zij op de hoogte gesteld van de manier waarop de gemeente met hun persoonsgegevens om zal gaan. De betrokkene wordt niet nogmaals geïnformeerd als hij al weet dat de gemeente persoonsgegevens van hem verzamelt en verwerkt, en weet waarom en voor welk doel dat gebeurt.

  Wanneer de gegevens via een andere weg verkregen worden, dus buiten de betrokkene om, wordt de betrokkene geïnformeerd op het moment dat deze persoonsgegevens 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 is, 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 15 AVG). De gemeente zal zich er van vergewissen dat de betrokkene zich op adequate wijze identificeert voordat zij aan dit verzoek voldoet. Het recht van inzage is mede bedoeld om uitoefening van het recht op rectificatie, het recht op gegevenswissing en beperking van de verwerking mogelijk te maken.

- *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 treffen 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 overtollige persoonsgegevens te wissen. Er kan sprake zijn 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 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).

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

  Betrokkene mag vragen om een 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 wil niet 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.

- *Recht van bezwaar (artikel 21 AVG)*

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

  - Om reden van bijzondere persoonlijke omstandigheden;
  - Als sprake is van verwerking op basis van een publiekrechtelijke taak van een bestuursorgaan of;
  - Als sprake is van een verwerking op basis van een gerechtvaardigd belang (inclusief profilering).

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

  De betrokkene heeft desgevraagd het recht om zijn persoonsgegevens die hij aan de gemeente heeft verstrekt 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 verwerkingsverantwoordelijke rechtstreeks zijn persoonsgegevens doorstuurt naar de nieuwe verwerkingsverantwoordelijke.

- *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 betrokkenen

Om gebruik te maken van zijn 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 bestaat de mogelijkheid om bezwaar te maken bij de gemeente en om een klacht in te dienen bij de gemeente en/of de Autoriteit Persoonsgegevens. Hierover zal betrokkene geïnformeerd worden.

De te volgen procedure in geval van uitoefening van een recht zoals beschreven onder 5.1 wordt neergelegd in nadere procesbeschrijvingen.

5.3. Klachten

In het contact met de gemeente kan wel eens wat misgaan. Een betrokkene 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 Venlo 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. Mogelijke afwijkingen van beleidskader

Bij voorgenomen afwijkingen van het beleidskader door de burgemeester en/of de gemeentesecretaris laten zij zich adviseren door de FG.

7. Schema verantwoordelijkheden en borging

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

Verantwoordelijkheid	**Wie en hoe**
Vaststellen privacybeleid	De bestuursorganen van de gemeente Venlo (het college, de raad en de burgemeester) hebben het beleid vastgesteld en bevorderen de

	beschikbaarheid van voldoende middelen om privacybescherming passend te waarborgen.
Beheer van privacybeleid	De privacy officer beheert het beleid namens de portefeuillehouders, in samenspraak met de FG en portefeuillehouders[11] privacy. De teamleider/proceseigenaar rapporteert over wat de kwaliteit is van de uitvoering van het beleid aan directie/portefeuillehouder. De FG ziet hier op toe en adviseert waar nodig de directie, het college, de raad en burgemeester en doet aanbevelingen voor verdere optimalisering. Waarborg voor optimalisering is het hanteren van de PDCA-cyclus.
Uitvoering van privacybeleid	Er zijn door de bestuursorganen portefeuillehouders privacy aangewezen. Deze zijn verantwoordelijk voor uitvoering van het privacybeleid alsmede voor controle op de naleving van afspraken. Het directieteam is verantwoordelijk voor de integrale sturing van de ambtelijke organisatie op naleving van het privacybeleid. Zij heeft uit haar midden een voor privacy verantwoordelijke directeur aangewezen. Teamleiders/proceseigenaren zijn verantwoordelijk voor implementatie van het privacybeleid binnen hun team en proces, en voor uitvoering van de hierin opgenomen normen. Zij worden hierin bijgestaan door de privacy officer en rapporteren hierover gevraagd en ongevraagd aan de FG.
Ontwikkeling en uitvoering van thematisch beleid	De portefeuillehouders privacy zien toe op de ontwikkeling en uitvoering van thematisch privacy beleid door teamleiders/proces-eigenaren. 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/ teamleider wordt hierin ondersteund door de privacy officer.
Bestuurlijke verantwoording	Jaarlijks legt het college verantwoording af aan de gemeenteraad over de status van de uitvoering van het privacybeleid, onder meer over de risico's en beheersmaatregelen.
Toezicht	De bestuursorganen hebben een FG aangesteld die toeziet op de naleving van privacywet- en regelgeving en privacybeleid. De FG rapporteert aan de bestuursorganen en onderhoudt de contacten met de Autoriteit Persoonsgegevens. De positie en taken van de FG zijn vastgelegd in artikel 38 en 39 AVG en nader uitgewerkt in het Statuut Functionaris Gegevensbescherming.
Monitorings- en verantwoordingsplan	De FG ziet er samen met de verantwoordelijke portefeuillehouders en in samenspraak met de concerncontroller op toe dat er een privacy monitorings- en verantwoordingsplan wordt ontwikkeld en dat dit wordt uitgevoerd. Dit plan wordt jaarlijks opgesteld. De PDCA-cyclus wordt hierop toegepast.
Risicogedreven aanpak	Vertrekpunt voor het maken van beleidskeuzes op procesniveau is de DPIA. In samenwerking met de privacy officer en na advies van de FG brengen teamleiders/proceseigenaren daarmee de mate van het

[11] Bij de raad vervuld de raadsgriffier zowel de rol van portefeuillehouder, directie als teamleider. Ten aanzien van de verwerkingen waarvoor de burgemeester verwerkingsverantwoordelijke is worden deze rollen vervuld door de kabinetschef.

	risico voor betrokkenen in kaart en worden passende maatregelen geformuleerd. De risico's en maatregelen worden voorgelegd aan het college[12] en het college besluit of en welke maatregelen worden uitgevoerd. Over de uitvoering van maatregelen rapporteert de teamleider/proceseigenaar aan directie/college. De FG houdt hierop toezicht en adviseert zonodig de directie/ college. De risico's worden door praktische, organisatorische en technische maatregelen beheerst en volgens de PDCA-cyclus geborgd.
Register van verwerkingen	De bestuursorganen zijn verantwoordelijk voor het aanleggen van een register van verwerkingen voor de verwerkingen waarvoor zij verwerkingsverantwoordelijke zijn. Teamleiders/proceseigenaren zijn verantwoordelijk voor het melden van nieuwe verwerkingen en relevante wijzigingen, waarna deze in het register verwerkt worden. In een interne procedure is de wijze van beheer van, en controle en toezicht op dit register vastgelegd.
Meldplicht datalekken	De verantwoordelijkheden t.a.v. de meldplicht datalekken zijn vastgelegd in de interne procedure meldplicht datalekken, genaamd de procedure meldplicht datalekken.
Convenanten, verwerkersovereenkomsten en geheimhoudingsverklaringen	Daar waar samengewerkt wordt met externe partijen, of aan externe partijen of personen opdracht gegeven wordt om persoonsgegevens te verwerken zijn de proceseigenaren/ teamleiders verantwoordelijk voor het aangaan van convenanten, verwerkersovereenkomsten en geheimhoudingsverklaringen. Zij worden hierin ondersteund door de privacy officer.
Bewustwording	De teamleiders/proceseigenaren zorgen ervoor dat medewerkers regelmatig getraind worden en dat actief ingezet wordt op bewustmaking ten aanzien van privacy. De FG en privacy officer ondersteunen daarbij en zien daarop toe.
Privacy services	Teamleiders/proceseigenaren zijn verantwoordelijk voor correcte en transparante afwikkeling van verzoeken van betrokkenen. Zij rapporteren hierover aan de FG. De privacy officer ondersteunt teamleiders/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 zal de klachtbehandelaar afstemming zoeken met de FG.

8. 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[13].

De privacy officer is in de uitvoerende zin eigenaar van het privacybeleidskader en daarmee verantwoordelijk voor het beheer en onderhoud ervan.

[12] Respectievelijk de raad of burgemeester indien het verwerkingen betreft waarvoor zij verantwoordelijk zijn.
[13] Zie artikel 24 lid 1 en 2 AVG

Het privacybeleidskader wordt na verloop van drie jaar 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.