Privacybeleid gemeente Leudal

Inhoudsopgave

1. Inleiding

Privacy speelt een belangrijke rol in de relatie tussen de burger en de overheid en staat daarmee hoog op de bestuurlijke agenda. Gemeenten hebben de verantwoordelijkheid over persoonsgegevens en gegevensuitwisseling van alle terreinen waarop ze actief zijn. Alle betrokkenen moeten er op kunnen vertrouwen dat de gemeente op een zorgvuldige en veilige, proportionele en vertrouwelijke wijze omgaat met het verzamelen, bewaren en beheren van persoonsgegevens van burgers. Dat geldt onder andere voor taken op het gebied van basisadministraties, openbare orde en veiligheid, en het sociaal domein. Goed en zorgvuldig omgaan met persoonsgegevens is een dagelijkse bezigheid van gemeenten. Het beschermen van de privacy is complex en wordt steeds complexer door technologische ontwikkelingen, de decentralisaties en kent grote uitdagingen op het gebied van veiligheid en de Europese privacywetgeving. Daarom is het belangrijk om transparant te zijn over de wijze waarop de organisatie omgaat met persoonsgegevens en het waarborgen van de privacy van haar burgers.

1.1 Wat is privacy?

In de Nederlandse Grondwet is privacy omschreven als het recht op eerbiediging van de persoonlijke levenssfeer, artikel 10 Grondwet. De kern van het recht op eerbiediging van de persoonlijke levenssfeer (privacy) is de bescherming van het recht op persoonlijke vrijheid en individuele autonomie, zowel in relatie tot de overheid in de afbakening van de privé sfeer, als in relatie tot de rechten en vrijheden van anderen. Kernpunten inzake de verwerking van persoonsgegevens daarbij zijn: 1) rechtmatig, behoorlijk en transparant, 2) doelbinding en verenigbaarheid, 3) gegevensminimalisatie, 4) juistheid, 5) opslagbeperking, 6) integriteit en vertrouwelijk en 7) verantwoordingsplicht.

Privacy geldt voor alle processen van de gemeente en heeft betrekking op het politieke bestuur, alle medewerkers, burgers, gasten en externe relaties.

1.2 Missie, visie en ambitie privacy

Privacy maakt integraal deel uit van de organisatiestrategie. Het beschermen van persoonsgegevens heeft een steeds grotere rol binnen de bedrijfsvoering. Privacy dient daarbij vastgelegd te worden in alle ambities die de gemeente nastreeft.

Missie

Gemeente Leudal wil voldoen aan wet- en regelgeving. Dit betreft de Algemene Verordening Gegevensbescherming en de Uitvoeringswet AVG.

Visie

De medewerkers van de gemeente Leudal hebben voldoende kennis om proactief op ontwikkelingen in de werkprocessen te anticiperen. Waarbij aangetoond wordt dat privacy is geborgd in de processen.

Ambitie

Aantoonbaar maken dat privacy is geborgd in alle werkprocessen.

Om de borging van privacy te kunnen waarborgen vergt dit een goede werkwijze, 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. Het goed inregelen van alle benodigde facetten om privacy te borgen geeft geen garantie dat er nooit een datalek of andere calamiteit met persoonsgegevens zal voorkomen. Maar mocht het gebeuren, dan wordt nagenoeg de kans uitgesloten dat dit voorkomt door onrechtmatig en onbehoorlijk bestuur.

De ambitie van de gemeente Leudal rondom het borgen van privacy is dan ook het kunnen aantonen dat privacy is geborgd in alle werkprocessen die de organisatie kent.

1.3 Doel en toepassingsbereik van het beleid

Het doel van dit privacybeleid is om kaders vast te leggen waarmee gewaarborgd wordt dat de gemeente Leudal op een behoorlijke en zorgvuldige wijze persoonsgegevens verwerkt in overeenstemming met de wet. Met dit beleid wil de gemeente Leudal dus inzichtelijk maken op welke wijze zij dagelijks omgaat met persoonsgegevens in relatie tot verschillende wetten en verdragen waarin de bescherming van privacy is geregeld. Dit privacybeleid is in lijn met de relevante nationale en Europese wet- en regelgeving.

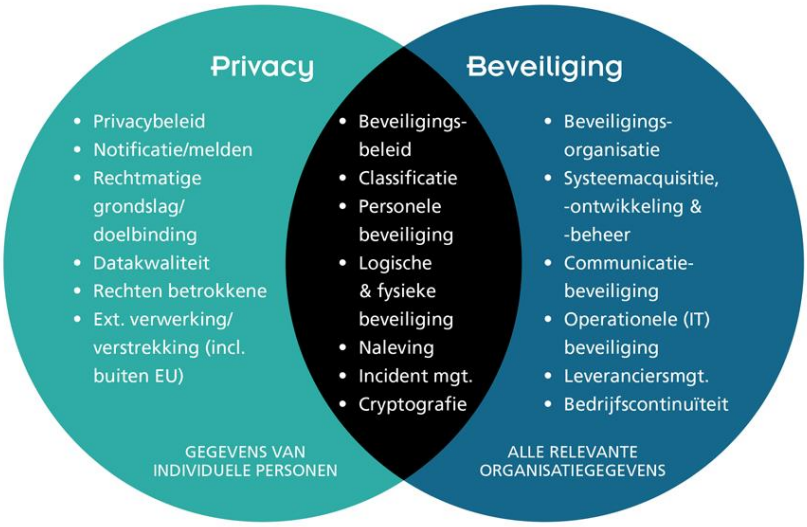
Het beleid is van toepassing op alle verwerkingen van persoonsgegevens door alle bestuursorganen van de gemeente. Het beleid heeft, net zoals de AVG, géén betrekking op de verwerking van gegevens over rechtspersonen c.q. in de gemeente Leudal gevestigde ondernemingen, zoals de naam en de rechtsvorm van de rechtspersoon en de contactgegevens van de rechtspersoon.

1.4 Samenhang privacy en informatiebeveiliging en andere raakvlakken

Er is een nauwe samenhang tussen privacy en informatiebeveiliging. Het zijn twee verschillende begrippen, maar wel met een gemeenschappelijk raakvlak. Privacy gaat over het vertrouwelijk omgaan met persoonlijke gegevens en het voldoende beschermen hiervan. Informatiebeveiliging gaat over de beschikbaarheid, integriteit en vertrouwelijkheid van alle (gevoelige) informatie. Zowel informatiebeveiliging als privacy vragen om een risico-gedreven aanpak.

Het privacybeleid kan door deze samenhang niet los worden gezien van het informatiebeveiligingsbeleid. De visie in dit privacybeleid komt overeen met de visie opgenomen in het informatieveiligheidsbeleid (i-visie). Het informatiebeveiligingsbeleid van de gemeente Leudal voldoet aan de landelijk gestelde beveiligingsnormen voor de overheid en is opgenomen in het Strategisch Informatieveiligheidsbeleid 2020-2022, welke zijn vertaald in het Tactisch Informatieveiligheidbeleid.

De afbeelding hieronder geeft de samenhang weer.



Tekstversie afbeelding privacy en beveiliging

Privacy

Dit begrip heeft betrekking op de gegevens van individuele personen en omvat onderwerpen zoals:

- Privacybeleid
- Notificatie/melden
- Rechtmatige grondslag/doelbinding
- Datakwaliteit
- Rechten betrokkene
- Ext.verwerking/verstrekking (inclusief buiten EU)

Beveiliging

Dit begrip heeft betrekking op alle relevante organisatiegegevens en omvat onderwerpen zoals:

- Beveiligingsorganisatie
- Systeemacquisitie,-ontwikkeling & beheer
- Communicatiebeveiliging
- Operationele(IT) beveiliging
- Leveranciersmgt
- Bedrijfscontinuïteit

Gemeenschappelijk raakvlak

- Beveiligingsbeleid
- Classificatie
- Personele beveiliging
- Logische & fysieke beveiliging
- Naleving
- Incident mgt
- Cryptografie

1.4.1 Archief en gegevensvernietiging

Het archiefbeleid van de gemeente Leudal is vastgelegd in de Archiefverordening gemeente Leudal 2020 en het Besluit informatiebeheer gemeente 2020. Hierin zijn tevens bepalingen opgenomen omtrent gegevensvernietiging, welke zijn gebaseerd op de Archiefwet. In de privacywetgeving is het een verplichting om een duidelijke termijn af te spreken hoe lang persoonsgegevens worden bewaard, waarbij opslagbeperking het uitgangspunt is.

1.4.2 Integriteit

Het veilig omgaan met persoonsgegevens vereist een integere houding. Om hiervoor aan de voorkant bewustzijn te creëren, leggen nieuwe medewerkers van de gemeente Leudal de eed of belofte af en dienen zij een geheimhoudingsverklaring te ondertekenen. Alle externen welke werkzaamheden verrichten voor de gemeente Leudal tekenen vooraf een geheimhoudingsverklaring. Dit is vastgelegd in het Proces 'In- Door- en Uitstroom (IDU).

2 Wettelijke kaders

Sinds 25 mei 2018 is de Europese Verordening 'The General Data Protection Regulation' (GDPR) van kracht. In Nederland is deze verordening vertaalt in de Algemene verordening gegevensbescherming (AVG), ook wel de Europese Privacywetgeving genoemd. Het doel van de AVG is om de bescherming van natuurlijke personen in verband met de verwerking van hun gegevens en het vrije verkeer van persoonsgegevens binnen de Europese Unie te waarborgen.

De AVG heeft rechtstreekse werking binnen de gehele Europese Unie en harmoniseert daarmee de regels voor de bescherming van persoonsgegevens. Echter, op specifieke punten biedt de AVG lidstaten de ruimte om nadere invulling te geven aan bepalingen uit de AVG. Deze invulling geschiedt via zogenaamde uitvoeringswetten, zoals in Nederland de Uitvoeringswet AVG. De belangrijkste gebieden waar de Uitvoeringswet AVG een rol in speelt zijn:

1. het toepassingsbereik van de AVG;
2. de rol, positie en bevoegdheden van de nationale toezichthouder (AP);
3. regelingen rondom het gebruik van bijzondere categorieën van persoonsgegevens;
4. regelingen omtrent (de uitzonderingen op de rechten van betrokkenen) en;
5. regelingen voor specifieke verwerkingssituaties (zoals in relatie tot de vrijheid van meningsuiting).

Voorts staan in specifieke wetten aanvullende of meer specifieke eisen en kaders voor een bepaalde sector of domein. Zoals de Wet maatschappelijke ondersteuning 2015 (Wmo), de Jeugdwet of de wet Basisregistraties Personen (wet BRP).

2.1 Belangrijke definities

Omdat de volgende begrippen veel in het privacybeleid worden gebruikt, worden deze nader uitgewerkt. Indien de begrippen reeds zijn opgenomen in de AVG (artikel 4), zal hier aansluiting bij worden gezocht:

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

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

Persoonsgegevens: Alle gegevens die gaan over mensen en waaraan je een mens als individu kunt herkennen. Het gaat hierbij niet alleen om vertrouwelijke gegevens, zoals over iemands gezondheid, maar om ieder gegeven dat te herleiden is tot een bepaald persoon (bijvoorbeeld; naam, adres, geboortedatum). Naast gewone persoonsgegevens kent de wet ook bijzondere persoonsgegevens. Dit zijn gegevens die gaan over gevoelige onderwerpen, zoals etnische achtergrond, politieke voorkeuren of het Burgerservicenummer (BSN).

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

Verwerkingsregister: Het register dat wordt bijgehouden door de verwerkingsverantwoordelijke, waarin de categorieën van verwerkingen van persoonsgegevens organisatie worden bijgehouden. De Functionaris Gegevensbescherming is intern verantwoordelijk voor het bijhouden van het verwerkingsregister.

Verwerkingsverantwoordelijke: Een persoon of instantie die alleen, of samen met een ander, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.

Verwerking: Een verwerking is alles wat je met een persoonsgegeven doet, zoals: 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.

2.2 Specifieke beleidsterreinen

2.2.1 Sociaal domein

De nieuwe taken die de gemeente in het sociaal domein sinds 1 januari 2015 in uitvoering heeft genomen, gaan gepaard met de verwerking van, veelal bijzondere, persoonsgegevens van nieuwe klantgroepen.

2.2.1.1 Overleg over cliënten

Efficiency, effectiviteit en kwaliteit van de dienstverlening zijn er mee gebaat dat daar waar nodig en mogelijk, zowel intern als extern afstemming over een cliënt plaatsvindt tussen de verschillende onderdelen van het sociaal domein. Ondanks dat dit ook een van doelstellingen is van de wetgever, heeft de wetgever de informatie-uitwisseling in het kader van de afstemming niet geregeld. Participatiewet, Jeugdwet en WMO 2015 kennen daarvoor ieder hun eigen regels.

Dit houdt in dat vanuit de algemene uitgangspunten van de AVG gegevens dienen te worden uitgewisseld en met name de beginselen van:

- transparantie (wees altijd transparant naar betrokkenen toe);
- proportionaliteit en dataminimalisatie (niet meer dan nodig);
- subsidiariteit (alleen indien nodig, kan het ook op een andere wijze?);
- niet langer dan nodig (denk aan de bewaartermijnen).

Binnen het sociaal domein zijn hierover werkafspraken gemaakt. Van belang is hier te wijzen op de komst van de Wet Aanpak Meervoudige problematiek Sociaal domein (Wams). Met de komst van de Wams zal de wettelijke lacune in deze worden opgevuld en zal er helderheid komen over gegevensuitwisselingen binnen het sociaal domein alsook het hergebruik van gegevens in geval van meervoudige problematiek.

2.2.1.2 De verbinding tussen openbare orde en veiligheid en sociaal domein

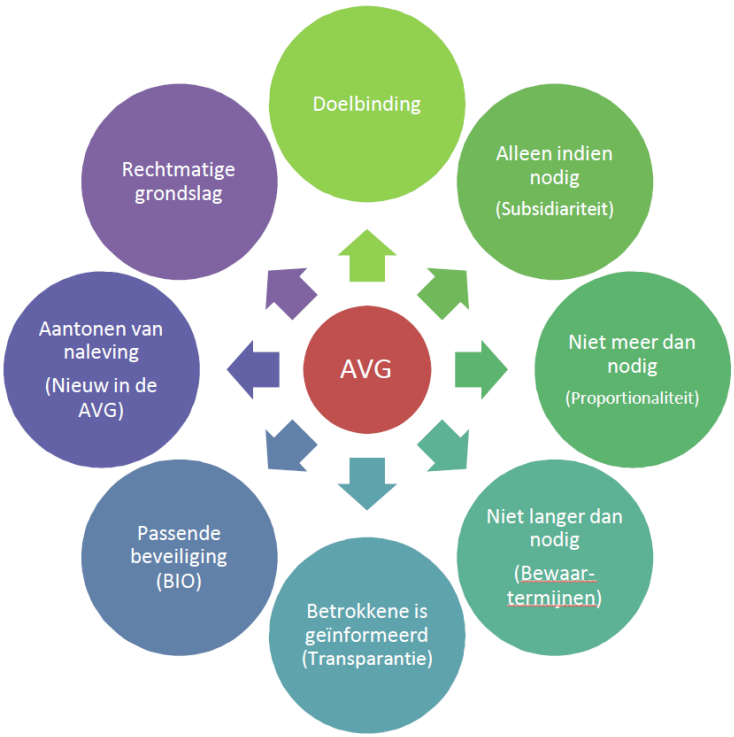
De afgelopen jaren is de gemeente Leudal meer persoonsgegevens gaan verwerken van personen die een bedreiging (kunnen) vormen voor de openbare orde en veiligheid. Het oplossen van problemen met (potentiële) overlastgevers is steeds vaker een bestuurlijke in plaats van een politionele aangelegenheid en gegevens van politie en justitie worden meegenomen in casus overleggen in het sociaal domein. De uitwisseling van dergelijke gegevens vindt plaats binnen de wettelijke mogelijkheden van verwerking van persoonsgegevens.

2.2.2 Openbaarheid van Bestuur

Publicatie van persoonsgegevens op internet wordt tot het uiterste beperkt. In de eerste plaats dient te worden afgewogen of aan publicatie van persoonsgegevens (spontaan zowel als op verzoek) niet valt te ontkomen. Als publicatie onontkoombaar is, dan wordt afgewogen of het publicatiemiddel internet het kanaal is waarlangs gepubliceerd wordt. De gemeente Leudal hanteert daarbij als uitgangspunt de Richtsnoeren voor actieve openbaarmaking en de Richtsnoeren inzake de publicatie van persoonsgegevens op internet. Mocht publicatie van persoonsgegevens op internet noodzakelijk zijn, dan zullen die gegevens worden afgeschermd voor zoekmachines.

3. Beginselen

De gemeente Leudal is verplicht om enkele beginselen bij de verwerking van persoonsgegevens in acht te nemen (artikel 5 AVG). De gemeente Leudal gaat op een zorgvuldige manier om met persoonsgegevens en respecteert daarbij de privacy van betrokkenen. Hieronder worden puntsgewijs de beginselen uitgewerkt waar de gemeente Leudal zich aan dient te houden bij het verwerken van persoonsgegevens:



Tekstversie afbeelding beginselen van de AVG

- Doelbinding
- Alleen indien nodig (subsidiariteit)
- Niet meer dan nodig (proportionaliteit)
- Niet langer dan nodig (bewaartermijnen)
- Betrokkene is geïnformeerd (transparantie)
- Passende beveiliging(BIO)
- Aantonen van naleving (nieuw in de AVG)
- Rechtmatige grondslag

3.1 Rechtmatig, behoorlijk, transparant (sub a)

Rechtmatig

De gemeente Leudal gaat zorgvuldig om met de persoonsgegevens die zij verwerkt. Dit noemen we rechtmatigheid. Een verwerking is alleen rechtmatig indien en voor zover aan de voorwaarden is voldaan zoals opgenomen in artikel 6 AVG, te weten:

- wanneer de betrokkene toestemming heeft gegeven voor de specifieke verwerking (sub a);
- voor de uitvoering van een overeenkomst waar de betrokkene onderdeel was (sub b);
- om een verplichting na te komen die in de wet staat (sub c);
- om een ernstige bedreiging voor de gezondheid van de betrokkene te bestrijden (sub d);
- voor de goede invulling van de gemeentelijke taak (sub e);
- indien een zorgvuldige belangenafweging dit uitwijst (sub f).

De gemeente Leudal verwerkt persoonsgegevens zoveel als mogelijk vanuit de publieke taak welke zij heeft op grond van aan haar opgelegde taken. De rechtmatigheid wordt ook vertaald in specifieke werkprocessen en procedures, zonder dat dit in het geding komt van de werkbaarheid.

Behoorlijk

Behoorlijk en zorgvuldig omgaan met persoonsgegevens, betekent ook dat we niet meer gegevens verwerken dan nodig. Dit noemen we dataminimalisatie of gegevensminimalisatie.

Dit sluit ook aan bij de principes van subsidiariteit en proportionaliteit. Dit betekent dat we het verwerken van persoonsgegevens - wat gezien kan worden als een inbreuk in de privacy van de betrokkene - zo klein mogelijk houden en dit in verhouding staat tot het bereiken van het doel waarvoor de persoonsgegevens verwerkt worden.

Soms is per wet bepaald welke gegevens noodzakelijk zijn om het doel te bereiken. In andere

gevallen maakt de gemeente Leudal deze afweging zelf. Hierbij worden alleen de gegevens verwerkt die nodig zijn om het doel te bereiken. Waar mogelijk wordt gewerkt met anonieme gegevens.

Transparant

De gemeente Leudal 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 dat doet. Overeenkomstig het transparantiebeginsel moeten informatie en communicatie in verband met de verwerking van die persoonsgegevens eenvoudig toegankelijk en begrijpelijk zijn, en moet duidelijke en eenvoudige taal worden gebruikt. De gemeente Leudal zorgt ervoor dat betrokkenen worden geïnformeerd over de doeleinden van de verwerkingen. Vaak gebeurt dit al doordat de betrokkene zijn/haar gegevens zelf doorgeeft op een aanvraagformulier. Hierop staat vaak al vermeld welke persoonsgegevens nodig zijn en voor welk doel. Als de gemeente persoonsgegevens verwerkt die ze niet van de betrokkene krijgt, stelt ze de betrokkene op de hoogte.

3.2 Doelbinding en verenigbaar (sub b)

De gemeente verwerkt alleen persoonsgegevens voor een doel waar een grondslag voor is. De AVG kent zes grondslagen die de verwerking van persoonsgegevens rechtvaardigen, zie artikel 6 AVG. Persoonsgegevens worden gebruikt voor het doel waarvoor ze zijn verzameld en eventuele verenigbare doelen. De gemeente Leudal herbruikt deze persoonsgegevens niet voor andere doelen

3.3 Gegevensminimalisatie (sub c)

Gegevensminimalisatie wordt ook wel dataminimalisatie genoemd. Het betekent dat de gemeente niet meer persoonsgegevens mag verzamelen dan strikt noodzakelijk is voor het beoogde doel (proportionaliteitsbeginsel).

3.4 Juistheid (sub d)

Alle redelijke maatregelen moeten worden genomen om ervoor te zorgen dat onjuiste persoonsgegevens worden gerectificeerd of gewist.

3.5 Opslagbeperking (sub e)

Er dient te worden gezorgd dat de opslagperiode (oftewel de bewaartermijn) van de persoonsgegevens tot een strikt minimum worden beperkt. Wanneer er nog persoonsgegevens opgeslagen zijn die niet langer nodig zijn voor het bereiken van het doel worden deze zo snel mogelijk verwijderd. Dit houdt in dat deze gegevens vernietigd worden, of zo worden aangepast dat de informatie niet meer gebruikt kan worden om iemand te identificeren.

Om ervoor te zorgen dat persoonsgegevens niet langer worden bewaard dan noodzakelijk is, stelt de gemeente termijnen vast voor het wissen van gegevens of voor een periodieke toetsing ervan.

Hoe lang de gemeente Leudal persoonsgegevens bewaart, loopt uiteen. De Archiefwet en diverse andere wetten, verplichten de gemeente om gegevens voor een minimale of maximale termijn te bewaren. Tijdens deze bewaartermijn zorgt de gemeente voor een zorgvuldige en veilige opslag. Na verloop van de verplichte bewaartermijn worden de gegevens vernietigd.

3.6 Integriteit en vertrouwelijkheid (sub f)

Integriteit en vertrouwelijkheid

De gemeente Leudal gaat zorgvuldig om met persoonsgegevens en behandelt deze vertrouwelijk. Zo worden persoonsgegevens alleen verwerkt door personen die een geheimhoudingsplicht hebben ondertekend. Daarbij zorgt de gemeente Leudal voor passende beveiliging van persoonsgegevens, waarvoor de kaders zijn vastgelegd in het informatiebeveiligingsbeleid.

Passende beveiliging

Persoonsgegevens moeten worden verwerkt op een manier die een passende beveiliging en vertrouwelijkheid van die gegevens waarborgt, ook ter voorkoming van ongeoorloofde toegang tot of het ongeoorloofd gebruik van persoonsgegevens en de apparatuur die voor de verwerking wordt gebruikt.

Voor gemeenten geldt de Baseline Informatiebeveiliging Overheid (BIO) als verplichtende voorwaarden om te voldoen aan het begrip Passende beveiliging. In het strategisch informatieveiligheidsbeleid is hier verdere invulling aan gegeven waar hier naar wordt verwezen.

3.7 Privacy by design en privacy by default

Privacy by design

De gemeente Leudal richt haar werkprocessen zo in dat ze voldoen aan de in dit beleid gestelde kaders en uitgangspunten. Dit noemen we privacy by design. Door vooraf na te denken over mogelijke privacyvraagstukken en dit mee te nemen in de inrichting van de processen en systemen, verkleinen we eventuele privacyrisico's.

Privacy by default

Daar waar dit mogelijk is worden de instellingen van de applicaties dusdanig ingesteld dat zoveel mogelijk rekening wordt gehouden met de bescherming van de rechten van personen. Dit houdt in dat daar waar dit mogelijk is niet meer gegevens worden gedeeld/getoond dan noodzakelijk is voor de uitoefening van de taken. Hierop zal middels logging en controles op de logging worden toegezien.

4. Verantwoordelijkheden en rollen bij de naleving

Ingevolge artikel 5, tweede lid, AVG is de verwerkingsverantwoordelijke verantwoordelijk voor de naleving van de beginselen inzake de verwerking van persoonsgegevens zoals uitgewerkt in hoofdstuk 3. De Autoriteit Persoonsgegevens (AP) is de toezichthoudende instantie in Nederland die er toezicht op houdt dat de verantwoordelijke ook daadwerkelijk de AVG naleeft en de persoonsgegevens beschermt. De AP kan (extra) onderzoek doen en heeft de mogelijkheid bestuursmaatregelen en boetes op te leggen indien de AVG niet wordt nageleefd.

Maar wie in de organisatie is nu verantwoordelijk voor de naleving van privacy wet- en regelgeving en welke rol speelt eenieder hierin?

4.1 Verantwoordingsplicht

Alle bestuursorganen van de gemeente zijn verantwoordelijk voor de naleving van de privacy wet- en regelgeving, zoals de AVG en het privacybeleid, ieder voor zover het haar bestuurlijke taken betreft. De bestuursorganen van de gemeente zijn de gemeenteraad, het College van Burgemeester en Wethouders (het college van B&W) en de burgemeester.

Wanneer de verwerking van persoonsgegevens van rechtswege gedelegeerd is aan externe organisaties die daarbij ook zelf doel en middelen kunnen bepalen, zijn de bestuursorganen van deze organisatie zelf verwerkersverantwoordelijke (en dus verantwoordelijk voor de naleving van de privacy) in de zin van de AVG.

4.2 Borgen van de naleving

Het borgen van de bescherming van persoonsgegevens is een taak van eenieder in de organisatie. De gehele organisatie is immers betrokken bij de verwerking van persoonsgegevens. Het bestuur, de gemeentesecretaris/algemeen directeur, de proceseigenaren en de procesbeheerders spelen een cruciale rol bij het uitvoeren van dit privacybeleid. Het management maakt, mede naar aanleiding van een inschatting van de risico's die de gemeente Leudal hierin loopt, de inschatting van het belang van de verschillende delen van het privacy.

4.3 Verschillende rollen

Om daadwerkelijk te kunnen waarborgen dat privacybescherming ingebed wordt in de organisatie is het noodzakelijk dat alle in de organisatie werkzame personen (inclusief externen en inhuur), ieder vanuit hun eigen rol worden bezien. Hieronder worden deze verschillende rollen en verantwoordelijkheden om uitvoering te geven aan dit privacybeleid kort aan de orde gesteld.

4.3.1 Gemeenteraad

De gemeenteraad heeft een toezichthoudende rol op basis van de controlerende taak die de Gemeentewet aan hen toekent.

4.3.2 College van B&W en burgemeester

Het college van B&W en de burgemeester zijn, ieder voor zover het haar of zijn bevoegdheid betreft, integraal (bestuurlijk) verantwoordelijk voor de beveiliging van informatie en de borging van privacy binnen de werkprocessen van de gemeente Leudal. Zij stellen kaders op voor informatieveiligheid en de bescherming van privacy op basis van Europese en landelijke wet- en regelgeving en daaraan gerelateerde normenkaders. Dit wordt vastgesteld in het informatieveiligheidsbeleid, het privacybeleid en de privacyverklaring. In een aantal specifieke bij wet bepaalde gevallen ligt deze bevoegdheid bij de burgemeester in plaats van bij het college.

Zowel het college van B&W als de gemeenteraad (controle functie) kunnen opdracht geven om controle te laten uitvoeren. Het college van B&W legt verantwoording af aan de Raad. Ook melden zij bijzonderheden ten aanzien van gegevensverwerking proactief aan de gemeenteraad. Te denken valt aan ernstige datalekken.

Privacy wordt geborgd door middel van een vaste plek in het college, met een vaste portefeuillehouder die de tijd, de kennis en de bestuurskracht heeft om in te grijpen in alle onderdelen van de organisatie en haar processen waar de zorgvuldigheid van persoonsgegevens in het geding is.

4.3.3 De gemeentesecretaris/algemeen directeur

De gemeentesecretaris/ algemeen directeur heeft eveneens een belangrijke rol in het borgen van privacy. De gemeentesecretaris/algemeen directeur:

- zorgt dat alle processen en systemen en de daarbij behorende middelen altijd onder de verantwoordelijkheid vallen van een afdelingshoofd/proceseigenaar, procesbeheerder en systeemeigenaar;
- stuurt op concernrisico's ten aanzien van informatieveiligheid en privacy;
- ziet er op toe dat informatiebeveiligings-onderwerpen een onderdeel zijn van de
- P&C-gesprekken en dat risicovolle onderwerpen worden opgenomen in de auditplannen.

4.3.4 De afdelingshoofden en teamleiders

De afdelingshoofden vormen samen het management, welke een gezamenlijk standpunt innemen over onder andere de missie, visie en ambitie van het privacybeleid. Teamleiders zijn de schakel tussen het management en de medewerkers welke uitvoering geven aan de processen. De afdelingshoofden en teamleiders zijn dan ook een belangrijke schakel in het bewaken dat de wet- en regelgeving wordt nagestreefd en voelen zich hier verantwoordelijk voor. Zij zorgen ervoor dat:

- er voldoende bewustwording is omtrent privacy en informatieveiligheid en deze twee onderwerpen als vast onderdeel op de agenda komen te staan. Voor de bewustwording worden zij uiteraard bijgestaan door de PO (privacy) en de CISO (informatieveiligheid).
- er in ieder team een medewerkers als privacy-ambassadeur is aangewezen.
- de medewerkers in hun team het privacybeleid uitvoeren en adequate maatregelen nemen om de risico's te beperken;
- de benodigde mensen en middelen beschikbaar worden gesteld om hun afdelings-/teamprocessen te kunnen uitvoeren overeenkomstig dit beleid;
- de operationele procedures/ werkplannen voor de verwerkingen in hun afdeling/team worden opgesteld en dat het management deze vaststelt;
- gecontroleerd wordt of de getroffen maatregelen overeenstemmen met de gestelde eisen en of deze voldoende bescherming bieden om te voldoen aan de privacywetgeving;
- de verantwoordelijke portefeuillehouders binnen het college gevraagd en ongevraagd worden geïnformeerd over de borging en naleving van het privacybeleid binnen de organisatie.
- Het afdelingshoofd Dienstverlening zorgt dat het privacybeleid, wat in overeenstemming is met het informatiebeveiligingsbeleid, wordt opgesteld.

4.3.5 De Functionaris Gegevensbescherming (FG)

Conform de verplichting uit artikel 37 AVG heeft de gemeente een FG aangesteld voor het houden van onafhankelijk controle en toezicht op de wijze waarop de organisatie invulling geeft aan maatregelen om aan de privacy wet- en regelgeving en informatiebeveiliging te voldoen. De taken van de FG staan beschreven in artikel 39 AVG en zijn, kort samengevat:

- verwerker en verwerkersverantwoordelijke informeren en adviseren over hun verplichtingen uit hoofde van de AVG;
- toezien op naleving van de AVG;
- desgevraagd advies verstrekken met betrekking tot DPIA's en toezien op de uitvoering daarvan;
- samenwerken met en het optreden als contactpersoon van de AP en;
- bewustwording creëren over de privacywetgeving.

Een nieuwe verwerking van persoonsgegevens wordt eerst aan de FG gemeld voordat de verwerking begint, zodat hij kan bepalen of hier eerst een DPIA voor dient te worden uitgevoerd.

De FG is verantwoordelijk voor het structureel toetsen van de implementatie en de uitvoering van de wettelijke eisen en de gemeentelijke richtlijnen op het gebied van privacy. De FG werkt nauw samen met de CISO en de PO en dient als eerste aanspreekpunt te fungeren voor vraagstukken van de CISO en de PO.

De FG dient eveneens goed bereikbaar te zijn voor burgers waarvan wij persoonsgegevens verwerken of andere externe partijen waar de gemeente samenwerkingen mee heeft. Burgers en externe partijen kunnen vragen stellen over de verwerking van persoonsgegevens door de organisatie of (vermoedens) van misbruik van persoonsgegevens door onze organisatie doorgeven. De FG is bereikbaar via het speciale emailadres: fg@leudal.nl.

4.3.6 De Privacy Officer (PO)

De Privacy Officer fungeert als aanspreekpunt voor privacyvraagstukken die spelen in de organisatie. Hij adviseert over en werkt mee aan het beleid/visie van de gemeente op het gebied van privacy en werkt mee aan het verhogen van het privacy-bewustzijn binnen de organisatie.

Hij adviseert de organisatie over privacy vraagstukken van de organisatie en behandelt de ingekomen privacy verzoeken. Ook ondersteunt en adviseert de PO organisatiebreed over privacy en (het verwerken van) persoonsgegevens. Het is hierbij niet de bedoeling dat de PO de taken op het gebied van bescherming van de privacy van de teams overneemt. De teams hebben hun eigen verantwoordelijkheid in het goed omgaan met privacygevoelige gegevens.

De PO zorgt ervoor dat de wettelijk verplichte taken uit hoofde van privacy wet- en regelgeving worden uitgevoerd en dat maatregelen worden ingebed in de organisatie. De PO werkt hiervoor nauw samen met de CISO en de FG.

4.3.7 De Chief Information Security Officer (CISO)

De Chief Information Security Officer ondersteunt en adviseert de organisatie en de proceseigenaren en procesbeheerders bij het bewaken en verhogen van de betrouwbaarheid van de informatievoorziening. Hij heeft gemeentebreed de regie op het proces van informatieveiligheid en houdt kwaliteit en tijdigheid in beeld en doet voorstellen over mogelijke en/of noodzakelijke bijsturing. Hij rapporteert hierover rechtstreeks aan de gemeentesecretaris/algemeen directeur.

Hij stelt het informatiebeveiligingsbeleid en de ontwikkelplannen op. Deze zijn gebaseerd op een risicomanagement-benadering en hierbij is rekening gehouden met het informatiebeveiligingsdreigingsbeeld, de trends en de organisatiebehoefte. De CISO werkt nauw samen met de PO en de FG.

De CISO is de ENSIA- coördinator. De ENSIA coördinator heeft een toezichthoudende en controlerende taak en is verantwoordelijk voor het tijdig insturen van alle ENSIA audits. De CISO is aangewezen als eerste Vertrouwde Contactpersoon Informatiebeveiliging (VCIB).

4.3.8 Privacy-ambassadeur

Privacybescherming en informatiebeveiliging onderbrengen bij één afdeling doet geen recht aan het onderwerp. Om een hogere bewustwording in de gehele organisatie te creëren en te behouden, is per team een medewerker als privacy-ambassadeur aangewezen. De privacy-ambassadeur draagt, in samenwerking met het afdelingshoofd /teamleider en de FG, PO en CISO, zorg voor een doorlopende bewustwording over privacy (en informatieveiligheid) binnen zijn team. De privacy-ambassadeur spant zich in:

- voor het bijhouden en doorgeven van nieuwe verwerkingen van zijn team en wijzigingen in bestaande verwerkingen van zijn team waarbij persoonsgegevens worden gebruikt ten behoeve van het up-to-date houden van het verwerkingsregister van de gemeente. Deze wijzigingen geeft hij door aan de PO, die de verantwoordelijkheid draagt voor het up-to-date houden van het verwerkingsregister organisatiebreed.
- voor het leveren van een bijdrage aan het creëren van meer bewustwording, in ieder geval tijdens het bespreken van het vaste onderwerp tijdens de teamoverleggen. Ook zal hij het team op de hoogte brengen van nieuwe ontwikkelingen binnen het privacyrecht, waarbij hij ondersteund wordt door de PO.
- nieuwe medewerkers in zijn team op de hoogte te brengen van de privacyregels, waarbij in ieder geval onderhavig privacybeleid en het Protocol Datalekken onder de aandacht wordt gebracht.

4.3.9 Privacyteam en datalekteam

Om ervoor te zorgen dat de organisatie zich aan de privacyregels houdt en de informatie in de organisatie is beveiligd, is vaak veel kennis en kunde nodig. Daarvoor zijn verschillende disciplines nodig en dienen verschillende afdelingen aangehaakt te worden.

De sleutelfunctionarissen van het privacyteam en het datalekteam zijn: de FG, de CISO en de PO. Ze hebben wekelijks een overleg om elkaar op de hoogte te houden van hetgeen er speelt binnen de organisatie op het gebied van privacy en informatieveiligheid. Ook brengen ze elkaar op de hoogte van de nieuwe ontwikkelingen, waarbij de FG vanuit zijn rol het voortouw neemt.

De interne organisatie kan het team bereiken door de speciale emailadressen die hiervoor in het zijn ingesteld: privacy@leudal.nl en datalekken@leudal.nl.

De privacy-ambassadeurs kunnen in hun rol de PO ondersteunen om een privacybewuste organisatie te worden en te blijven. De privacy-ambassadeurs sluiten minimaal eens per kwartaal aan bij het privacy-team-overleg, met als voornaamste doel kennisoverdracht en bespreking van een plan van aanpak betreffende het optimaliseren van doorlopende bewustwording binnen de teams.

Onmisbare schakel in het datalekteam is ICT. Door de juiste beveiligingsmaatregelen te treffen op de ICT-infrastructuur van de gemeentelijke organisatie kunnen beveilingsincidenten en datalekken worden voorkomen. Eens per jaar wordt samen met ICT het protocol Datalekken doorlopen en zo nodig een oefening gedaan.

De FG houdt vanuit zijn rol de gemeentesecretaris/ algemeen directeur op de hoogte en, op verzoek, rapporteert hij hem over de ontwikkelingen en afspraken welke worden gemaakt in de teams en de voortgang hiervan.

4.3.10 Medewerkers

Alle medewerkers (inclusief inhuur/externen) zijn verantwoordelijk voor de bescherming van de privacy van betrokkenen en het goed en zorgvuldig verwerken van persoonsgegevens. Dat betekent dat iedere medewerker, binnen de kaders van zijn rol/functie, zorgt voor een rechtmatige, behoorlijke en transparante verwerking van persoonsgegevens. Medewerkers zorgen dat privacy is opgenomen in hun werkprocessen waarin persoonsgegevens een rol spelen. Wanneer ze twijfels hierover hebben, schakelen zij hiervoor de hulp in van de PO (voor de borging van de privacy) en CISO (voor de zorg rondom de informatiebeveiliging).

5. Inbedding in de organisatie

Zoals gezegd heeft de gemeente een verantwoordingsplicht om een belangrijke bijdrage te leveren aan de bescherming van het grondrecht van mensen betreffende privacy. De gemeente Leudal moet aantonen dat een verwerking aan de belangrijkste beginselen van privacy zoals opgenomen in hoofdstuk 3 van dit beleid voldoet. De gemeente heeft hiervoor de volgende stappen ondernomen.

5.1 Register van verwerkingen

Om de naleving van de AVG aan te kunnen tonen, houdt de gemeente Leudal een register bij van alle verwerkingsactiviteiten waarvan de gemeente de verwerkingsverantwoordelijke is. Het betreft een verplichting welke voortvloeit uit artikel 30 AVG. Het register van verwerkingen wordt ook wel het verwerkingsregister genoemd. Elk register bevat een beschrijving van wat er tijdens een verwerking plaatsvindt, en welke gegevens daarvoor worden gebruikt, namelijk:

- de naam en contactgegevens van de verwerkingsverantwoordelijke en, mogelijk, de
- gezamenlijke verwerkingsverantwoordelijke (sub a);
- de doelen van de verwerking (sub b);
- een beschrijving van het soort persoonsgegevens en de daarbij horende betrokkenen (sub c);
- een beschrijving van de ontvangers van de persoonsgegevens (sub d);
- een beschrijving van het delen van persoonsgegevens aan een derde land of internationale organisatie (sub e);
- de termijnen waarin de verschillende persoonsgegevens moeten worden gewist (sub f) en;
- een algemene beschrijving van de beveiligingsmaatregelen (sub g).

Het verwerkingsregister van de gemeente Leudal is een levend document, welk doorlopend up-to-date wordt gehouden met de nieuwste verwerkingen van persoonsgegevens. Het verwerkingsregister wordt online gepubliceerd. De laatste versie van het verwerkingsregister van de gemeente Leudal is te vinden op de gemeentelijke website.

5.2 Meldplicht datalekken

We spreken van een datalek wanneer persoonsgegevens in handen vallen van derden die geen toegang tot die gegevens mogen hebben. Voorbeelden hiervan zijn het kwijtraken van een USB-stick of papieren dossier met persoonsgegevens, inbraak door een hacker of het verlenen van autorisaties aan onbevoegden in het gemeentelijk systeem en het aan iemand (schriftelijk of digitaal) toezenden van persoonsgegevens die niet voor de ontvanger zijn bestemd. Indien een (vermoeden van) een datalek zich voordoet, dient de gemeente snel en efficiënt te handelen. Nagegaan moet worden of alle passende technische en organisatorische maatregelen zijn genomen om vast te stellen of een inbreuk in verband met persoonsgegeven heeft plaatsgevonden, en om de AP en de betrokkene daarvan onverwijld in kennis te stellen.

Wanneer er een datalek heeft plaatsgevonden, meldt de gemeente ingevolge artikel 33 AVG, dit zonder onredelijke vertraging, uiterlijk 72 uur nadat er kennis van de inbreuk is vernomen, aan de AP. Als dit later dan 72 uur is wordt er een motivering voor de vertraging bij de melding gevoegd. De kennisgeving kan ertoe leiden dat de AP optreedt overeenkomstig haar in de AVG neergelegde taken en bevoegdheden.

Bij het vaststellen van een datalek wordt onder meer de vraag nagegaan of de persoonsgegevens al dan niet waren beschermd door adequate en technische maatregelen die de kans op identiteitsfraude of andere vormen van misbruik beperkten. Wanneer wordt geconstateerd dat de inbreuk een hoog risico met zich meebrengt voor de rechten en vrijheden van de betrokkene(n), meldt de gemeente ingevolge artikel 34 AVG dit zonder onredelijke vertraging aan de betrokkenen in eenvoudige en duidelijke taal. De kennisgeving dient zowel de aard van de inbreuk in verband met persoonsgegevens te vermelden als aanbevelingen over hoe de natuurlijke persoon in kwestie mogelijke negatieve gevolgen kan beperken.

Om toekomstige datalekken te voorkomen worden bestaande datalekken geëvalueerd. De gemeente heeft tevens een 'Procedure datalek gemeente Leudal' vastgesteld.

Daarnaast worden er met opdrachtnemers en andere externe partijen die persoonsgegevens verwerken verwerkersovereenkomsten gesloten waarin afspraken staan over hoe de privacy van de persoonsgegevens moeten worden beschermd en hoe moet worden gehandeld bij een constatering van een (vermoedelijke) datalek.

5.3 Persoonsgegevens delen met derden

Sommige doelen worden bereikt door samenwerking tussen meerdere (maatschappelijke) organisaties. Hiervoor kan het nodig zijn om persoonsgegevens met elkaar te delen. Wanneer er persoonsgegevens met andere organisaties gedeeld worden, gebeurt dat altijd binnen de kaders en uitgangspunten zoals gesteld in dit beleid.

Wanneer de gemeente voor een verwerking met persoonsgegevens samenwerkt met partners of haar taken laat uitvoeren door een andere organisatie (dus een verwerker inschakelt), dient de gemeente voorzorgsmaatregelen te treffen om de bescherming van de privacy te waarborgen. Daarom wordt er met een samenwerkende partij een convenant gesloten en met een derde/onderneming die verwerkingen verwerkt een verwerkersovereenkomst, waarin afspraken worden vastgelegd over het verwerken van persoonsgegevens. Wanneer een externe/inhuur uit hoofde van zijn functie geacht wordt namens de gemeente persoonsgegevens te verwerken, dient hij daarvoor vóóraf een geheimhoudingsverklaring te ondertekenen.

Het aangaan van een convenant of een verwerkersovereenkomst geeft de mogelijkheid erop toe te zien dat ook door de andere partij (samenwerkende partij of verwerker) zorgvuldig wordt omgegaan met persoonsgegevens en een passende bescherming is gewaarborgd. Afdelingshoofden/ teamleiders zijn ervoor verantwoordelijk dat de gestelde eisen in de contracten worden geborgd en hierop wordt gecontroleerd.

De gemeente hanteert het door de VNG vastgestelde standaardmodelverwerkersovereenkomst. Het aangaan van een verwerkersovereenkomst betreft een vast onderdeel van het aanbestedings- en inkoopbeleid van de gemeente Leudal.

5.4 Data Protection Impact Assessment (DPIA)

Met een Data Protection Impact Assessment (DPIA), ook wel gegevensbeschermingseffectbeoordeling genoemd, worden de effecten en risico's van nieuwe of bestaande verwerkingen beoordeeld op de bescherming van de privacy. Het is een verplichting welke voortvloeit uit artikel 35 AVG om de naleving van de AVG te verbeteren indien de verwerking een hoog privacyrisico oplevert voor de burgers van wie de gemeente gegevens verwerkt. Bij de DPIA worden met name de oorsprong, de aard, het specifieke karakter en de ernst van dat risico van het verwerken van persoonsgegevens vooraf geëvalueerd door de verwerkersverantwoordelijke.

De gemeente voert in ieder geval een DPIA uit wanneer er wanneer er de volgende verwerking plaatsvindt:

- een geautomatiseerde verwerking (waaronder profilering);
- een grootschalige verwerking van persoonsgegevens of verwerking van strafrechtelijke gegevens of;
- wanneer er een grootschalige monitoring van openbare ruimten (cameratoezicht) plaatsvindt.

Dit geldt in het bijzonder bij verwerkingen waarbij nieuwe technologieën worden gebruikt, waarbij de DPIA altijd uitgevoerd dient te worden vóórdat met de verwerking wordt begonnen.

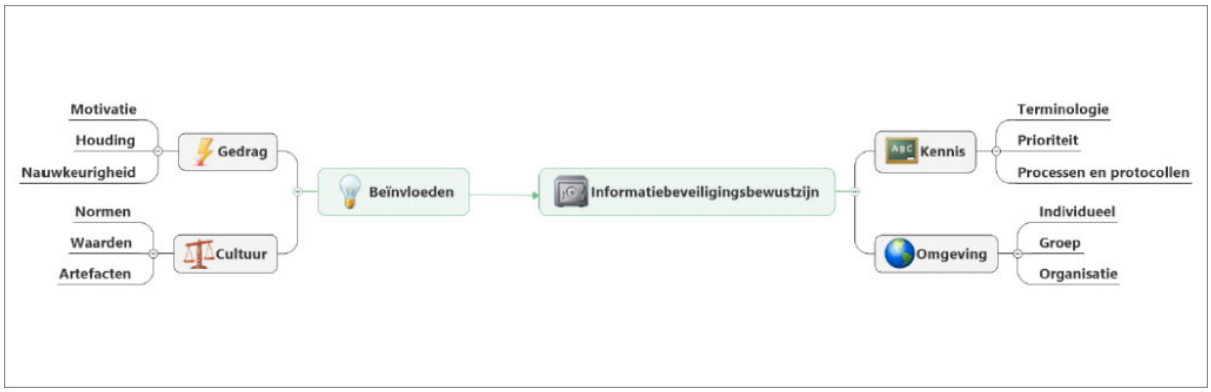
De gemeente hanteert een lijst van verwerkingen die op basis van risicobeoordeling leidt tot een eenvoudige, middelgrote en complexe DPIA. Aan de hand van de op dat moment actuele ontwikkelingen, wordt de keuze gemaakt welke DPIA wordt uitgevoerd.

5.5 Privacybewuste organisatie

Bewustwording is het sluitstuk van privacy wet- en regelgeving. Zoals in hoofdstuk 4 al eerder is aangegeven, is privacy een onderwerp wat de gehele organisatie aangaat. Als iedereen in de organisatie bewust is van zijn eigen verantwoordelijkheid op het gebied van privacy, draagt dit ook bij aan verbetering van bescherming van persoonsgegevens in zijn algemeen.

De media staat vol met berichten over datalekken, veelal veroorzaakt door menselijke fouten. Door het creëren van bewustwording over informatieveiligheid en privacy kan dit worden teruggedrongen. Bewustzijn hangt samen met vier aspecten:

- Gedrag: te beïnvloeden door te sturen op motivatie, houding en nauwkeurigheid.
- Cultuur: te beïnvloeden door te sturen op normen, waarden en artefacten.
- Kennis: bewustzijn creëren van terminologie, prioriteit en processen en protocollen.
- Omgeving: bewustzijn creëren van individueel, groep en organisatie.



Kennis van het onderwerp (wat houdt het in en hoe moet ermee om worden gegaan) kan worden gemeten door toetsing en onderzoek. Er kan gecontroleerd worden of alle richtlijnen en protocollen aanwezig zijn en voldoen aan de privacy wet- en regelgeving. Gedrag en cultuur zijn belangrijke aspecten die de bewustwording beïnvloeden. Door te voorkomen dat er een gebrek aan motivatie en nauwkeurigheid bij medewerkers ontstaat, zal gedrag en cultuur een positieve bijdrage leveren aan het borgen van de privacy en informatieveiligheid en tevens een verlaging van een risico op inbreuk van rechten.

Een privacybewuste organisatie komt alleen tot stand als alle medewerkers op hun eigen niveau kennis hebben van de regels over het omgaan met persoonsgegevens. Privacy-bewustzijn is dan ook een continu proces binnen de gemeente Leudal, waarbij kennis wordt overgedragen zodat zorgvuldig omgaan conform de beginselen van de AVG wordt aangemoedigd en voortdurend wordt verbeterd. Het privacybeleid wordt onder de aandacht gebracht bij bestaande en nieuwe medewerkers. De gemeente zorgt daarom voor een doorlopend aanbod van bewustwording op dit onderwerp. Hiervoor is een communicatieplan opgesteld om de bewustwording van privacy en informatieveiligheid te vergroten. Maar van de medewerkers wordt ook verwacht dat zij zich inspannen om deze kennis in de praktijk in te brengen.

6. Geautomatiseerde verwerkingen

Drie bijzondere vormen van geautomatiseerde verwerkingen van persoonsgegevens die in dit hoofdstuk aan de orde worden gesteld zijn: "profilering", "Big Data en tracking" en "inzet van camera's". Deze vormen zijn bijzonder te noemen om deze vorm van geautomatiseerd verwerken veelal een hoger gelegen doel dient.

6.1 Profilering (Artikel 22, AVG)

Profilering vindt plaats wanneer er een geautomatiseerde verwerking van persoonsgegevens plaatsvindt waarbij aan de hand van persoonsgegevens naar bepaalde persoonlijke aspecten van een persoon wordt gekeken om deze persoon te categoriseren en te analyseren, of om zaken te kunnen voorspellen. Voorbeelden van persoonlijke aspecten kunnen zijn; financiële situatie, interesses, gedrag of locatie.

Om profilering wat duidelijker te maken gebruiken we het volgende voorbeeld:
Wanneer een bezoeker op de gemeentelijke website naar een bepaalde dienst kijkt, mag de gemeente geen actie ondernemen om de dienst aan te bieden. Gemeenten mogen wel bekijken hoe vaak een bepaalde dienst bekeken is, maar dus niet specifiek gericht adverteren. Daarnaast geeft de wet aan dat er geen besluit mag worden genomen op basis van profilering.

De gemeente Leudal maakt alleen gebruik van profilering als dat past binnen de kaders van de privacy wet- en regelgeving.

6.2 Big Data en tracking

Door middel van Big Data onderzoek en tracking mogen alleen gegevens verwerkt worden wanneer deze niet herleidbaar zijn tot een natuurlijk persoon. Daarnaast worden ze alleen verzameld voor onderzoek dat door, of namens, de gemeente Leudal wordt uitgevoerd.

De verzamelde gegevens door Big data onderzoek en tracking zijn alleen de gegevens die door geautoriseerde personen zijn verzameld. Wanneer de gegevens worden omgezet in een dataset zal dataminimalisatie worden toegepast. Dit betekent dat alleen de data die echt nodig zijn voor het behalen van het doel gebruikt zullen worden. Daarnaast kunnen persoonsgegevens gepseudonimiseerd worden zodat zij niet herleidbaar zijn tot een persoon.

Gemeente Leudal maakt geen gebruik van tracking. Het gebruik van Big Data wordt op dit moment niet toegepast, maar er wordt wel onderzocht welke voordelen het gebruik van Big Data kan hebben voor onze dienstverlening. Daarbij wordt wel rekening gehouden met wat uiteengezet wordt in dit beleid. Voordat hier toe wordt overgegaan zal er een DPIA, inclusief privacy by design, worden uitgevoerd. Dit is bij big data en tracking van uiterst belang, omdat hierbij snel onbewust de regels rondom de verwerking van persoonsgegevens kunnen worden overtreden.

6.3 Inzet van camera's

Binnen de gemeente kan onder bepaalde omstandigheden gebruik worden gemaakt van cameratoezicht, zoals vastgelegd in de Gemeentewet. Cameratoezicht kan onder andere worden gebruikt voor het vergroten van de veiligheid op straat. Camera's kunnen een grote inbreuk maken op de privacy van diegenen die gefilmd worden. Om de privacy zo goed mogelijk te waarborgen worden camera's alleen ingezet wanneer er geen andere manieren zijn om het doel te bereiken, en worden er eisen gesteld aan de inzet van camera's.

7. Opvragen van informatie van persoonsgegevens

Informatie over persoonsgegevens moet overeenkomstig het transparantiebeginsel dat bestemd is voor het publiek of voor de betrokkene beknopt, eenvoudig toegankelijk en begrijpelijk zijn en moet duidelijk en in eenvoudige taal en, in voorkomend geval, aanvullend gevisualiseerd worden gebruikt. De gemeente verstrekt de informatie die tot het publiek is gericht voornamelijk via de website. Ook hanteert de gemeente een privacyverklaring, waarin - naast het verstrekken van informatie - persoonsgegevens via elektronische weg kunnen worden opgevraagd.

7.1 Recht op informatie

Een ieder heeft verschillende manieren om informatie op te vragen bij de overheid.

7.1.1 Wet openbaarheid van bestuur (Wob)

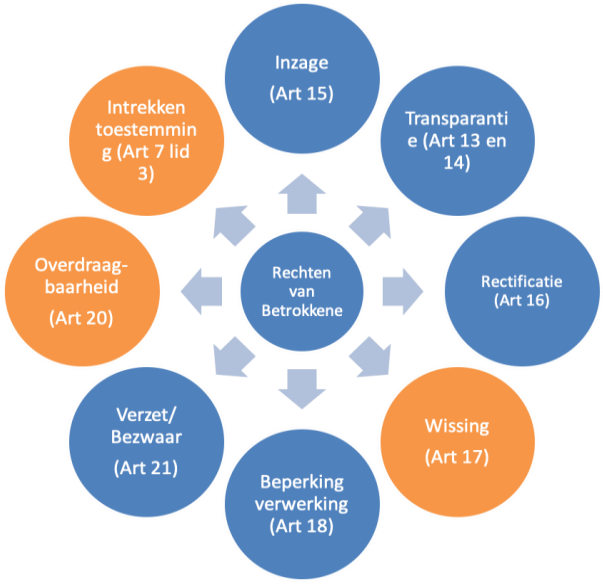
Via de Wob (en straks wellicht de Wet Open Overheid) kan een verzoek om informatie worden ingediend bij de gemeente. Bij het verzoek bekijkt de gemeente altijd of het antwoord geen inbreuk maakt op de persoonlijke levenssfeer van betrokkenen. Het uitgangspunt is dat er geen persoonsgegevens worden verstrekt.

7.1.2 Wet hergebruik van overheidsinformatie

De Wet hergebruik van overheidsinformatie regelt het op verzoek verstrekken van overheidsinformatie voor hergebruik. Bij het verzoek bekijkt de gemeente altijd of het antwoord geen inbreuk maakt op de persoonlijke levenssfeer van betrokkenen. Het uitgangspunt is dat er geen persoonsgegevens worden verstrekt.

7.1.3 Rechten van betrokkenen

De AVG kent betrokkenen verschillende privacyrechten toe om personen van wie de persoonsgegevens worden verwerkt controle te kunnen laten houden over hun persoonsgegevens. Deze rechten worden ook wel de rechten van betrokkenen genoemd en zijn terug te vinden in artikel 13 tot en met 22 AVG. De gegevens kunnen via een schriftelijk of via een webformulier, welke toegankelijk is via het gebruik van Digid. De rechten van betrokkenen zullen hieronder puntsgewijs worden toegelicht.



De blauw gekleurde bollen betreffen rechten die ook voor de komst van de AVG aanwezig waren: inzage (art.15), transparantie (art. 13 en 14), Rectificatie (art. 16), beperking verwerking (art.18) en verzet/bezwaar (art.21).
De oranje gekleurde bollen geven aan dat deze rechten nieuw zijn met de komst van de AVG: wissing (art.17), overdraagbaarheid (art.20) en intrekken toestemming (art.7 lid 3)

7.1.3.1 Recht op informatie (Transparantie)

Persoonsgegevens kunnen direct (dus van de betrokkene zelf) of indirect (niet van de betrokkene) zijn verkregen. De gemeente stelt de betrokkene op de hoogte van het feit dat verwerking van zijn persoonsgegevens plaatsvindt of zal plaatsvinden en wat de doeleinden daarvan zijn. In artikel 13 en 14 AVG is beschreven welke informatie in elk geval verstrekt moet worden. Wanneer het doel van de verwerking verandert, zal de gemeente de betrokkene hierover informeren.

Wanneer betrokkenen gegevens aan de gemeente geven, worden zij op de hoogte gesteld van de manier waarop de gemeente met persoonsgegevens om zal gaan. Dit kan bijvoorbeeld via een formulier gebeuren. Vaak staat op de aanvraagformulieren vermeld welke gegevens zonder toestemming niet openbaar gemaakt zullen worden. 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, wordt de betrokkene geïnformeerd op het moment dat deze voor de eerste keer worden verwerkt.

7.1.3.2 Recht op inzage

Betrokkenen hebben de mogelijkheid om te controleren of en op welke manier hun gegevens worden verzameld en verwerkt. In artikel 15 AVG staat een opsomming van informatie waarvoor het recht van inzage geld. Op verzoek van betrokkene wordt een kopie van de persoonsgegevens die worden verwerkt, verstrekt.

7.1.3.3 Recht op rectificatie

Als de gemeente persoonsgegevens van betrokkenen verwerkt die naar hun oordeel onjuist zijn, kunnen zij een verzoek indienen bij de gemeente om dit te verbeteren. Dit betreft een recht van de betrokkene welke is neergelegd in artikel 16 AVG. Het verzoek wordt uiteraard in behandeling genomen met inachtneming van de beperkingen zoals neergelegd in wet- en regelgeving. Wanneer daadwerkelijk rectificatie plaatsvindt, zal de gemeente iedere ontvanger aan wie persoonsgegevens zijn verstrekt in kennis stellen van deze rectificatie, tenzij dit onmogelijk is of onevenredig veel inspanning vraagt.

7.1.3.4 Recht om gegevenswissing / vergetelheid

Conform artikel 17 AVG hebben betrokkenen het recht om de gemeente te verzoeken bovenmatige persoonsgegevens te verwijderen, indien:

- persoonsgegevens niet langer nodig zijn voor de doeleinden waarvoor zij zijn verzameld of anderszins verwerkt (sub a);
- de betrokkene zijn toestemming intrekt en er geen andere rechtsgrond voor verwerking bestaat (sub b);
- betrokkenen bezwaar maakt tegen de verwerking en er zijn geen dwingende gerechtvaardigde gronden voor de verwerking die prevaleren (sub c);
- de persoonsgegevens onrechtmatig verwerkt zijn (sub d);
- de wet dwingt tot verwijdering (sub e) en;
- gegevens van kinderen zijn verzameld in het kader van diensten van informatiemaatschappij (sub f).

Het wissen van gegevens is niet altijd verplicht, bijvoorbeeld wanneer deze gegevens nodig zijn voor de doeleinden waarvoor ze zijn verwerkt.

7.1.3.5 Recht op beperking van de verwerking

Het recht op beperking houdt in dat de gemeente de persoonsgegevens (tijdelijk en onder voorwaarden) niet mag verwerken en niet mag wijzigen. Ingevolge artikel 18 AVG kan een betrokkene vragen om beperking van de verwerking in de volgende gevallen:

- de juistheid van de gegevens wordt door betrokkene betwist (sub a);
- de gegevens worden onrechtmatig verwerkt, maar de betrokkene niet wil dat de gegevens worden verwijderd (sub b);
- de doeleinden zijn vervallen, maar betrokkene heeft de gegevens nog nodig voor de instelling, uitoefening of onderbouwing van een rechtsvordering (sub c) en;
- in geval van een lopende bezwaarprocedure (sub d).

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

7.1.3.6 Recht op overdraagbaarheid/dataportabiliteit

Het recht op dataportabiliteit is neergelegd in artikel 20 AVG en houdt in dat een betrokkene het recht heeft zijn persoonsgegevens van een verwerkingsverantwoordelijke te verkrijgen in gestructureerde, gangbare en machineleesbare vorm. De gemeente is vanuit de AVG niet verplicht invulling te geven aan overdraagbaarheid van gegevens. Het recht op dataportabiliteit bestaat alleen wanneer de verwerking berust op toestemming of op een overeenkomst én de verwerking geautomatiseerd is. Desondanks zal de gemeente in voorkomende gevallen voorzieningen treffen in het kader van dataportabiliteit.

7.1.3.7 Recht op bezwaar

Een betrokkene heeft het recht om, vanwege redenen die verband houden met zijn specifieke situatie, aan de gemeente te vragen zijn persoonsgegevens niet meer te gebruiken en bezwaar (dat niet vergelijkbaar is met bezwaar op grond van de Awb) te maken tegen de verwerking van zijn persoonsgegevens (artikel 21 AVG). De gemeente moet hieraan voldoen, tenzij er gerechtvaardigde gronden zijn voor de verwerking.

7.1.3.8 Recht niet te worden onderworpen aan geautomatiseerde individuele besluitvorming/profilering

Uitgangspunt van artikel 22 AVG is dat er geen geautomatiseerde besluitvorming op basis van profilering mag plaatsvinden, als daaraan rechtsgevolgen voor de betrokkene (degene wiens persoonsgegevens het betreft) zijn verbonden of het besluit hem in aanmerkelijke mate treft. Daarbij kan gedacht worden aan bijvoorbeeld de kredietwaardigheid van een persoon. Een ander voorbeeld is het verwerken van sollicitaties via internet zonder menselijke tussenkomst.

In drie gevallen is geautomatiseerde individuele besluitvorming wel mogelijk (tweede lid). Dit is het geval wanneer:

- het noodzakelijk is voor de totstandkoming of de uitvoering van een overeenkomst (sub a);
- het toegestaan is bij een Unierechtelijke of lidstaatrechtelijke bepaling (sub b) en;
- het berust op de uitdrukkelijke toestemming van betrokkene (sub c).

7.2 Indienen van verzoek rechten van betrokkene

Om gebruik te maken van zijn/haar rechten kan de betrokkene een verzoek indienen. Dit verzoek kan schriftelijk worden ingediend of via een webformulier, welk toegankelijk is middels het gebruik van DigiD. De indiener van het verzoek dient zich altijd te legitimeren en kunnen aantonen dat de gegevens die de indiener wilt inzien, corrigeren of verwijderen daadwerkelijk van hem zijn. De gemeente heeft conform de AVG vier weken de tijd, vanaf de ontvangst van het verzoek, om te beoordelen of het verzoek gerechtvaardigd is. In complexe situaties kan deze termijn worden verlengd met twee extra maanden. In geval van overschrijding gelden de regels van de Algemene wet bestuursrecht (Awb).

7.3 Klacht over de verwerking van persoonsgegeven

Eenieder die in contact treedt met de gemeente kan zijn ongenoegen uiten over de wijze waarop een bestuursorgaan of een ambtenaar van de gemeente zich in een bepaalde aangelegenheid jegens een natuurlijk persoon of rechtspersoon heeft gedragen. Het betreft dan een klacht zoals bedoeld in artikel 9:1 van de Awb. Klachten worden behandeld conform de "Verordening Klachtbehandeling gemeente Leudal". Klachten worden altijd vertrouwelijk behandeld. Dit betekent dat de persoonsgegevens binnen de gemeentelijke organisatie alleen worden verstrekt aan diegenen die bij de klachtbehandeling betrokken zijn.

Wanneer de klacht gaat over het (vermoeden van) verwerking van betrokkene's eigen persoonsgegevens op een manier die in strijd is met de privacy wet- en regelgeving, dan zoekt de klachtencoördinator afstemming met de FG.

Ook kan de betrokkene (of diens gemachtigde) zijn of haar klacht in deze of een verzoek tot bemiddeling indienen bij de AP, Postbus 93374, 2509 AJ 's-Gravenhage. Volledigheidshalve wordt hierbij vermeld dat het hier niet gaat over de reguliere klachtenregeling aangaande het handelen en optreden van vertegenwoordigers van de gemeente.

8. Inwerkingtreding en citeertitel

Dit beleid is vastgesteld op 20 juli 2021 door het college van burgemeester en wethouders van gemeente Leudal en treedt in werking acht dagen nadat dit is bekendgemaakt, onder gelijktijdige intrekking van het op 16 juni 2015 bekendgemaakte privacybeleid gemeente Leudal.

Citeertitel

Dit beleid kan worden aangehaald als 'Privacybeleid gemeente Leudal'.

Heythuysen, 20 juli 2021

BURGEMEESTER EN WETHOUDERS VAN LEUDAL

De secretaris,

mr. drs. J.J.Th.L. Geraedts

De burgemeester

D.H. Schmalschläger