



Beleidskader veilig omgaan met persoonsgegevens van de gemeente Ede

Januari 2021

Beleidskader veilig omgaan met persoonsgegevens

1. Inleiding

Artikel 8 van het Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden luidt:
Right to respect for private and family life

1 Everyone has the right to respect for his private and family life, his home and his correspondence.

2 There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Artikel 10 van de Grondwet luidt:

1. Ieder heeft, behoudens bij of krachtens de wet te stellen beperkingen, recht op eerbiediging van zijn persoonlijke levenssfeer.

2 De wet stelt regels ter bescherming van de persoonlijke levenssfeer in verband met het vastleggen en verstrekken van persoonsgegevens.

3 De wet stelt regels inzake de aanspraken van personen op kennisneming van over hen vastgelegde gegevens en van het gebruik dat daarvan wordt gemaakt, alsmede op verbetering van zodanige gegevens.

In de Wet bescherming persoonsgegevens is verder uitwerking gegeven aan het grondrecht van eerbiediging van de persoonlijke levenssfeer. Het toezicht op de naleving van deze wet ligt bij de Autoriteit Persoonsgegevens. Door recente wetwijzigingen heeft de Autoriteit aan kracht gewonnen. Zo zijn de maximale boetebedragen die de Autoriteit kan opleggen sterk verhoogd en zijn organisaties die persoonsgegevens verwerken verplicht om datalekken te melden.

Inmiddels is bescherming van persoonsgegevens naar Europees niveau getild. Op 25 mei 2016 is de Algemene Verordening Gegevensbescherming (AVG) in werking getreden en zullen verwerkingsverantwoordelijken (waaronder gemeenten) vanaf 25 mei 2018 aan de Verordening moeten voldoen. De Wet bescherming persoonsgegevens zal deels worden overgeheveld naar de Uitvoeringswet Algemene Verordening Gegevensbescherming en voor het overige worden ingetrokken.

Dit beleidsplan geeft gemeentelijke invulling aan de AVG. Een belangrijk issue in de Verordening is het in lijn brengen van gemeentelijke taken waarbij persoonsgegevens worden verwerkt, het doel van de verwerking, de juridische grondslag voor de verwerking en de wijze waarop met een minimum aan persoonsgegevens het doel van de verwerking kan worden bereikt.

Voldoen aan de AVG betekent dat op verschillende terreinen binnen de gemeentelijke organisatie aandacht moet zijn voor privacy. Om die reden zullen governance, beleid, werkprocessen en triages, bewustwording en het beheer en opslag van gegevens in dit beleidsplan onder de loep genomen worden. Dit leidt mogelijk tot aanpassing van processen of werkafspraken of kan als leidraad worden gebruikt voor het maken van processen of werkafspraken over nieuwe verwerkingen. In dit beleidsplan zijn tevens de aanbevelingen uit het rekenkameronderzoek meegenomen.

In dit beleidsplan worden allereerst een aantal begrippen en het algemene kader voor gegevensverwerking besproken. Vervolgens zal dieper ingegaan worden in hoofdstuk 5 op governance, beleid in hoofdstuk 6, werkprocessen en triages in hoofdstuk 7, bewustwording in hoofdstuk 8 en tot slot in hoofdstuk 9 op beheer en opslag van persoonsgegevens.

Dit beleidsplan wordt iedere twee jaar herzien en indien de herziening aanleiding geeft tot wijzigingen stelt het college van burgemeester en wethouders deze wijzigingen vast.

2. Managementsamenvatting

Volgens de AVG is het college van burgemeester en wethouders verwerkingsverantwoordelijk en zijn zij gehouden aan de verordening te voldoen. Deze bestuurlijke verantwoordelijkheid zal voor de dagelijkse sturing worden belegd bij de verantwoordelijk portefeuillehouder.

In de praktijk is privacy een onderwerp dat op de werkvloer speelt. Uitgangspunt in dit beleidsplan is om de verantwoordelijkheid zo dicht mogelijk bij de werkvloer te organiseren door het mandateren van taken en bevoegdheden aan het afdelingsmanagement. Het mandaat behelst het geven van bevoegdheden en

middelen om zelfstandig per afdeling sturing te geven aan het privacybeleid. De concernadviseurs (de functionaris voor gegevensbescherming, de coördinator informatieveiligheid en de juridisch privacy-adviseur; specifieke taakinhoud in bijlage 1) bieden ondersteuning bij het inrichten van de kaders, zijn adviseurs voor technische en organisatorische kwesties, hebben een coördinerende rol in de bedrijfsvoeringscyclus en verwerken datalekken. De afdelingen zijn verantwoordelijk voor het inrichten van de interne processen, het opstellen van de juiste documenten (protocollen, werkprocessen e.d.) en de archivering van persoonsgegevens. Ook de taken en verantwoordelijkheden van de afdelingen zijn in bijlage 1 opgenomen.

De betrokkenheid van het college bij de vormgeving van het privacybeleid bestaat uit het jaarlijks vaststellen van activiteitenplannen (uit te werken in de werkinstructies) die per afdeling wordt gemaakt en een verantwoording over de inzet van middelen en het resultaat in het voorafgaande jaar.

De gemeente wil optimaal gebruik maken van de ruimte die de AVG biedt om persoonsgegevens te verwerken. Welke ruimte er precies is, wordt langzaam duidelijker door rechterlijke uitspraken, publicaties, opinies en stukken vanuit de Autoriteit Persoonsgegevens (AP). De gemeente handelt binnen de lijnen van de verordening, maar is (als de situatie daar om vraagt) bereid om risico te nemen om de grenzen van de verordening op te zoeken (zoals door middel van triages).

3. Begrippen

In dit beleidskader worden verschillende begrippen geïntroduceerd met een zekere lading vanuit de privacy-wetgeving. Het gaat hierbij om:

- 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 identicator zoals een naam, een identificatienummer, locatiegegevens, een online identicator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon;
- Bijzondere persoonsgegevens: alle persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen of het lidmaatschap van een vakbond blijken, en verwerking van genetische gegevens, biometrische gegevens met het oog op de, unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemand seksueel gedrag of seksuele gerichtheid.
- 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;
- 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;
- Verwerker: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/ dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt;
- Ontvanger: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, al dan niet een derde, aan wie/waaraan de persoonsgegevens worden verstrekt. Overheidsinstanties die mogelijk persoonsgegevens ontvangen in het kader van een bijzonder onderzoek overeenkomstig het Unierecht of het lidstatelijke recht gelden echter niet als ontvangers; de verwerking van die gegevens door die overheidsinstanties strookt met de gegevensbeschermingsregels die op het betreffende verwerkingsdoel van toepassing zijn;
- Derde: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, niet zijnde de betrokkene, noch de verwerkingsverantwoordelijke, noch de verwerker, noch de personen die onder rechtstreeks gezag van de verwerkingsverantwoordelijke of de verwerker gemachtigd zijn om de persoonsgegevens te verwerken;
- Toestemming van de betrokkene: elke vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee de betrokkene door middel van een verklaring of een ondubbelzinnige actieve handeling hem betreffende verwerking van persoonsgegevens aanvaardt;

4. Algemeen kader voor de verwerking van persoonsgegevens

Gemeenten hebben van oudsher de beschikking over een veelheid aan persoonsgegevens. Met deze persoonsgegevens dient zorgvuldig te worden omgegaan. Vanuit de Algemene Verordening Gegevensbescherming (AVG) geldt de verplichting dat het verzamelen van persoonsgegevens steeds gekoppeld moet zijn aan een bepaald doel, de doelbinding. Binnen de gemeentelijke organisatie worden voor verschillende doelen persoonsgegevens verwerkt.

4.1. Doelbinding

Uitgangspunt in de AVG is de verwerking van de persoonsgegevens. Deze verwerkingen worden gedaan in het kader van de taakuitoefening door medewerkers. Voor deze verwerkingen geldt dat er een doel geformuleerd moet worden waarvoor zij worden verwerkt.

De AVG laat in het midden hoe die doelen geformuleerd worden, Uitgangspunt van de verordening is dat persoonsgegevens voor een welbepaald, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld. De afdelingsmanager bepaalt in eerste instantie voor welke doelen zijn afdeling persoonsgegevens verwerkt bv vergunningverlening, subsidievaststelling of bepalen uitkering. Alle verwerkingen en hun doeleinden staan in het verwerkingsregister. Via het verwerkingsregister is er zicht op alle verwerkingsactiviteiten van de medewerkers en het doel waarvoor deze activiteiten plaatsvinden. Nieuwe verwerkingsactiviteiten of wijzigingen moeten in het verwerkingsregister worden opgenomen, met hun bijbehorende doel.

4.2. Toereikend, ter zake dienend en niet bovenmatig

Voor al deze afzonderlijke doeleinden dient vervolgens vastgesteld te worden welke persoonsgegevens hiertoe noodzakelijkerwijs verwerkt moeten worden. Uitgangspunt is dat het verwerken van persoonsgegevens toereikend, ter zake dienend en niet bovenmatig mag zijn. Toereikend wil zeggen dat op basis van de verwerking het juiste beeld gaat ontstaan. Ter verduidelijking; een winkelier, die een registratie bijhoudt van wanbetalers, zal een ontoereikende verwerking doen als deze niet tevens registreert of de betaling is opgeschort, omdat de klant een dispuut heeft over het product.

Ter zake dienend hangt nauw samen met het doel. Is het bijhouden door de winkelier bedoeld voor de administratie, dan kunnen de gegevens niet aangewend worden om het koopgedrag te analyseren. Bovenmatig tot slot hangt ook samen met het doel. Houdt de winkelier een registratie bij van wanbetalers voor zijn administratie, dan zal het registeren van de waarde niet bovenmatig zijn, het bijhouden van het aantal goederen mogelijk wel.

Voor de gemeente Ede geldt dat afdelingen per verwerking moeten vaststellen welke persoonsgegevens ten minste noodzakelijk zijn om het doel te kunnen bereiken.

4.3. Vereisten van doelmatigheid, proportionaliteit en subsidiariteit (het zakmes)

Naast de hiervoor genoemde beperkingen voor verwerking van persoonsgegevens gelden ook de eisen van proportionaliteit en subsidiariteit.

Het proportionaliteitsbeginsel houdt in dat de inbreuk op de belangen van de bij de verwerking van persoonsgegevens betrokkene niet onevenredig mag zijn in verhouding tot het met de verwerking te dienen doel. Anders gezegd; hoe verhoudt het doel van de informatieverzameling zich tegenover de schending van de persoonlijke levenssfeer van de betrokkenen. Ingevolge het subsidiariteitsbeginsel mag het doel waarvoor de persoonsgegevens worden verwerkt in redelijkheid niet op een andere, voor de bij de verwerking van persoonsgegevens betrokkene, minder nadelige wijze kunnen worden verwekelijkt (bv het verkrijgen van de informatie uit open data).

Ook hier wordt per activiteit beoordeeld of de verwerking doelmatig is, de inbreuk op de persoonlijke levenssfeer niet zwaarder weegt als de verwerking en of de persoonsgegevens ook op een andere wijze verkregen kunnen worden.

4.4. Grondslag

Om persoonsgegevens te mogen verwerken is het noodzakelijk dat er een geldige grondslag is op basis waarvan de gegevens mogen worden verwerkt. Artikel 6 AVG geeft hiertoe een limitatieve opsomming:

- Algemeen belang/openbaar gezag

- Wettelijke verplichting
- Gerechtvaardigd belang
- Uitvoering overeenkomst
- Toestemming
- Vitaal belang

Voor de verwerking van de persoonsgegevens is het noodzakelijk dat aansluiting gevonden kan worden bij een van deze grondslagen. Hierbij kan worden aangetekend dat de grondslag toestemming alleen gebruikt wordt als op grond van een van de andere grondslagen geen persoonsgegevens kunnen worden verwerkt en deze toestemming ondubbelzinnig kan worden gegeven door de betrokkene. Als op basis van een andere grondslag (voor de gemeente Ede zal dit in de regel een wettelijke verplichting of algemeen belang/openbaar gezag zijn) het mogelijk is gegevens te verzamelen, dan wordt geen toestemming aan de betrokkene gevraagd, tenzij een wettelijke bepaling daartoe verplicht.

4.5. Verwerkingsverantwoordelijke(n) en verwerker

In de AVG wordt onderscheid gemaakt tussen verwerkingsverantwoordelijke en verwerker.

De verwerkingsverantwoordelijke is de overheidsinstantie, dienst of ander orgaan die alleen of samen met anderen het doel en de middelen voor de verwerking van persoonsgegevens vaststelt. De verwerker is de overheidsinstantie, dienst of ander orgaan die ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt. Voorbeelden van verwerkers zijn ICT-dienstverleners of organisaties bij wie de gemeente Ede een aantal taken laat uitvoeren.

In de relatie verwerkingsverantwoordelijke en verwerker heeft laatstgenoemde geen zeggenschap over het doel en de middelen van de verwerking. Doel en middelen worden door de verwerkingsverantwoordelijke bepaald. Om te zorgen dat de verwerker zich richt naar de instructies van de verwerkingsverantwoordelijke en kan garanderen aan de verwerkingsverantwoordelijke dat het passende technische en organisatorische maatregelen heeft genomen om de rechten van betrokkenen te beschermen, wordt een verwerkersovereenkomst gesloten. De wetgever laat het in het midden of dit een aparte overeenkomst moet zijn of dat deze geïncorporeerd kan worden in de hoofdovereenkomst. Vanuit de VNG is een model-verwerkersovereenkomst uitgegeven welke wij als gemeente Ede toepassen.

Het is ook mogelijk dat twee of meer verwerkingsverantwoordelijken gezamenlijk het doel en de middelen van de verwerking bepalen. In die gevallen is het van belang dat op een transparante wijze de onderlinge verplichtingen zijn vastgelegd. Voor de gemeente Ede geldt dat als sprake is van een gezamenlijke verwerkingsverantwoordelijkheid dit vooraf is vastgelegd in een samenwerkingsovereenkomst aangevuld met een protocol voor gegevensbescherming.

4.6 Technische en organisatorische beveiliging

De verantwoordelijke legt passende technische en organisatorische maatregelen ten uitvoer om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. De maatregelen garanderen, rekening houdend met de stand der techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van te beschermen gegevens met zich meebrengen.

In de gemeente Ede wordt aan deze eis van passende maatregelen invulling gegeven door het invoeren van de maatregelen van de Baseline Informatiebeveiliging Overheid (BIO). Deze baseline is ontwikkeld door de Informatiebeveiligingsdienst (IBD) van de VNG. Met de implementatie van deze set worden de volgende zaken beoogd:

- het invoeren van een basisniveau van informatiebeveiliging: de set is zo opgezet en ingevuld dat met invoering van de maatregelen een minimaal beveiligingsniveau wordt gerealiseerd voor de meeste toepassingen. Deze maatregelen betreffen niet alleen ICT-technische maatregelen maar gaan ook over huisvesting, personeelsbeleid en -werving, contractmanagement, inkoop, voorlichting en bewustwording.
- het systematisch beoordelen van informatiesystemen en -verwerking op de beveiligings- en privacyrisico's en het zo nodig treffen van specifieke maatregelen bovenop het basis-beveiligingsniveau;
- het invoeren van een proces van plannen, uitvoeren, toetsen en bijsturen (PDCA) waarbij de maatregelen set systematisch gecontroleerd wordt op effectiviteit en zo nodig aangepast wordt om het passende beveiligingsniveau blijvend te kunnen waarborgen.

Het informatiebeveiligingsproces en de maatregelen van de BIO wordt in verschillende varianten binnen alle overheidsorganisaties gebruikt en zijn gebaseerd op de internationale beveiligingsstandaarden. ISO 270001 en ISO 270002

5. Governance

Om te voldoen aan de AVG zullen op bestuurlijk en ambtelijk niveau binnen de gemeente Ede een aantal organisatorische maatregelen noodzakelijk zijn. In paragraaf 5.1 en paragraaf 5.2 wordt de verdeling van bevoegdheden en verantwoordelijkheden geregeld tussen het bestuurlijke en ambtelijke niveau. Vanaf paragraaf 5.3 worden de functies benoemd die betrokken zijn bij het 'in control' brengen en houden van de gemeente Ede.

5.1. Privacy op bestuurlijk niveau

Binnen de kaders van de AVG is het college bestuurlijk eindverantwoordelijke voor de verwerking van persoonsgegevens. Deze gezamenlijke verantwoordelijkheid wordt belegd bij een van de wethouders die als vast aanspreekpunt fungeert voor privacy-issues.

Het college wil optimaal gebruik maken van de ruimte die de AVG biedt om persoonsgegevens te verwerken. Welke ruimte er precies is, wordt heel langzaam duidelijker. Dit betekent dat er een beleidsvrijheid is in het bepalen welke verwerkingen binnen de gemeente worden gedaan. Deze beleidsvrijheid wordt primair ingevuld door afdelingsmanagers. Onder omstandigheden kan het college uitdrukkelijk gevraagd worden in te stemmen met een verwerking. Het afwegingskader is de bescherming van de persoonsgegevens van inwoners afgezet tegen een belang van de gemeente, zoals veiligheid van medewerkers.

Een ander aspect waarbij privacy op bestuurlijk niveau een rol speelt is het besluitvormingsproces. Het besluitvormingsproces van het college speelt zich grotendeels in de openbaarheid af. Deze openbaarheid kan gaan knellen op het moment dat er in documenten persoonsgegevens staan. Om die reden zullen persoonsgegevens zoveel mogelijk buiten collegebesluiten gehouden worden, tenzij de betrokkene toestemming heeft gegeven. Slechts in uitzonderlijke gevallen mogen persoonsgegevens zonder toestemming openbaar gemaakt worden.

Mocht het toch noodzakelijk zijn om persoonsgegevens in stukken op te nemen die bestemd zijn voor het college, dan zal vooraf een afweging worden gemaakt over de geheimhouding. Bij voorkeur is er een versie met persoonsgegevens waarop geheimhouding wordt opgelegd. In de openbare versie worden de persoonsgegevens dan onleesbaar gemaakt. Als dit niet goed mogelijk is dan kunnen de persoonsgegevens ook worden opgenomen in een geheime bijlage of kan zelfs het hele document geheim worden gehouden.

Bij collegestukken zijn het collegebesluit en het voorblad openbaar. Soms worden bijlagen bij het voorstel openbaar bekendgemaakt (bijvoorbeeld een beleidsregel).

Bij raadsstukken zijn alle stukken openbaar, tenzij er geheimhouding is opgelegd. Het beleid van de gemeente Ede is er op gericht om geen persoonsgegevens in openbare stukken op te nemen, tenzij het een bewuste keuze is het wel te doen.

5.2 Privacy op ambtelijk niveau

De feitelijke verwerking van persoonsgegevens vindt plaats binnen de ambtelijke organisatie op afdelingsniveau. De uitwerking van de eindverantwoordelijkheid die het college draagt wordt ingevuld op dit niveau. Hier worden het doel en de middelen van de verwerking bepaald. Het is niet meer dan logisch dat een deel van de bevoegdheden en verantwoordelijkheden op het terrein van de privacy die ligt bij het college gemandateerd wordt naar afdelingsmanagers, zodat zij op effectieve wijze privacy in hun dagelijkse processen kunnen incorporeren.

Langs deze weg worden afdelingsmanagers primair verantwoordelijk om passende technische en organisatorische maatregelen treffen om de rechten van betrokkenen te waarborgen en de verwerking in overeenstemming te brengen met de AVG. Waar het gaat om het treffen van technische maatregelen of inwinnen van advies kan een beroep gedaan worden op informatiespecialisten en voor organisatorische (waaronder de vertaling van dit beleidskader naar afdelingsniveau) en juridische vraagstukken bij privacyadviseurs (juridisch privacy-adviseur en FG).

De afdelingsmanagers dragen er ook zorg voor dat medewerkers op de afdeling gehouden zijn tot geheimhouding van de persoonsgegevens waar zij kennis van nemen. Voor de ambtenaren die in vaste dienst zijn bij de gemeente geldt de ambtseed. Voor personen die niet in dienst zijn van de gemeente Ede, zoals gedetacheerde medewerkers of tijdelijke inhuur geldt dat zij een geheimhoudingsverklaring moeten tekenen.

Bij het aangaan van externe relaties (de verwerking gegevens vindt buiten de deur plaats, Trusted Third Parties, of de persoonsgegevens worden voor verdere verwerking overgedragen) vormt geheimhouding eveneens een belangrijk onderdeel. Voor dit doel wordt een verwerkersovereenkomst of een protocol afgesloten (zie voor het verschil verderop). De ondertekening van verwerkersovereenkomsten of protocollen vindt plaats in de ambtelijke lijn op afdelingsniveau of hoger. Om beheer en opslag te vereenvoudigen is het wenselijk om afspraken die in verwerkersovereenkomsten en protocollen staan op te nemen in de samenwerkingsovereenkomsten. Hierdoor wordt het sluiten van afzonderlijke overeenkomsten voor verwerking persoonsgegevens zoveel mogelijk vermeden.

De verantwoordelijkheid van de afdelingsmanager op privacygebied is gekoppeld aan mandaten vanuit het college met daarin bevoegdheden en middelen. Hierbij kan worden gedacht aan:

- bepalen van het doel en middel van de verwerking,
- alloceren middelen in termen van menskracht en geld,
- bepalen van (mede)verantwoordelijkheid voor de verwerking,
- voorbereiden van verwerkingsrelaties, protocollen en verwerkersovereenkomsten opstellen (al dan niet als onderdeel van de samenwerkingsovereenkomst),
- technische infrastructuur voor de verwerkingen,
- archivering,
- inzetten Data Protection Impact Assessment (DPIA) of soortgelijke instrumenten om de privacy te toetsen,
- waarborgen rechten betrokkenen,
- verwerkingen in het verwerkingsregister muteren en
- melden datalekken en andere incidenten.

Voor iedere afdeling geldt dat er privacy-acties zijn die (al dan niet doorlopend) uitgevoerd moeten worden. Opvolging van deze acties wordt tijdens de bedrijfsvoeringsgesprekken met afdelingsmanagers besproken.

Een belangrijke taak voor afdelingsmanagers is het bieden van zekerheid aan medewerkers. Voorkomen moet worden dat medewerkers door de druk van privacy niet tot verwerking overgaan, waar dat uit hoofde van hun professie wel wordt gevraagd (zoals het delen van gegevens met anderen om optimaal hulp te kunnen verlenen en een ergere situatie te voorkomen). De AVG is er niet op gericht het werken onmogelijk te maken, maar om de gemeente en medewerkers bewust met privacy om te laten gaan en compliant te worden. Uitgangspunt van compliance is dat medewerkers persoonsgegevens enkel verwerken voor de taak die zij uitvoeren en dat, als de situatie er om vraagt, verdere verwerking (zoals delen met collega's) kan, mits men dit kan motiveren en vastlegt in het dossier.

Zeker in het begin zijn fouten (met mogelijk datalekken tot gevolg) onvermijdelijk, echter afdelingsmanagers moeten op dit punt het vertrouwen blijven uitspreken in medewerkers en hen de gelegenheid bieden van casusposities te leren om compliance in de vingers te krijgen.

5.3 Functionaris voor gegevensbescherming

Op grond van artikel 37 AVG wordt een functionaris voor gegevensbescherming (FG) aangewezen. De verwerkingsverantwoordelijke draagt hierbij zorg dat de FG aangewezen wordt op grond van zijn professionele kwaliteiten en, in het bijzonder, zijn deskundigheid op het gebied van wetgeving en de praktijk inzake gegevensbescherming en zijn vermogen om de taken die met zijn functie samenhangen, genoemd in artikel 39 AVG, te vervullen.

De verwerkingsverantwoordelijke is op grond van artikel 37 AVG gehouden om de contactgegevens van de FG bekend te maken en mede te delen aan de Autoriteit Persoonsgegevens (AP). Binnen de gemeente Ede valt de FG formatief onder concern-control.

De wettelijke taken en bevoegdheden van de FG geven deze functionaris een onafhankelijke positie in de organisatie. De taken en verantwoordelijkheden van de FG zijn te vinden in bijlage 1.

Van resultaten uit audits en overige bevindingen doet de FG rechtstreeks verslag aan het college van burgemeester en wethouders van de gemeente Ede.

5.4 Klachtbehandeling

In geval van een schending van rechten van betrokkenen (zie paragraaf 6.1) moet een betrokkene, los van andere juridische middelen, een klacht kunnen indienen bij de gemeente Ede als verwerkingsverantwoordelijke.

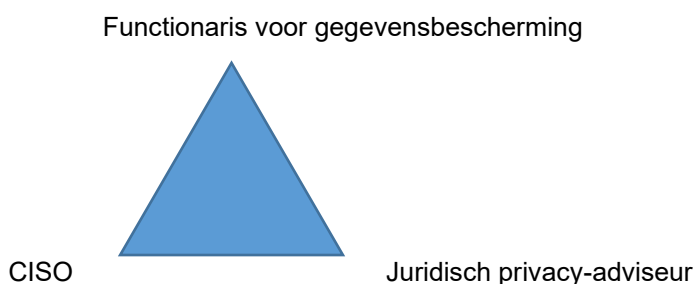
De gemeente Ede heeft een richtlijn voor klachtbehandeling. De klachtencoördinator zorgt dat een klacht over schending van privacyrechten bij de klachtbehandelaar terecht komt (meestal de afdelingsmanager).

5.5 Overige functies in kader van privacy

Buiten de in de AVG met naam genoemde functie van FG houden zich binnen de gemeente Ede ook anderen zich nadrukkelijk bezig met de dagelijkse praktijk rond privacy.

Organisatorisch wordt op twee niveaus uitwerking gegeven aan het privacybeleid; concern- en afdelingsniveau.

Op concernniveau vertaalt het zich in een driehoek bestaande uit de FG (vanuit CC), CISO (vanuit IPPM) en een juridisch privacy-adviseur (vanuit JIS).



Naast toezicht op naleving AVG ziet de FG tevens toe op informatieveiligheid, waarmee er op het gebied van informatieveiligheid een goede functiescheiding is gemaakt. Hierbij zorgt de coördinator informatieveiligheid er voor dat de juiste en passende beveiligingsmaatregelen gekozen, geïmplementeerd en geëvalueerd worden. De FG ziet toe op de werking van het proces en de maatregelen en brengt hier verslag van uit aan het management en bestuur.

De taken en verantwoordelijkheden van de juridisch privacy-adviseur binnen de gemeente Ede zijn terug te vinden in bijlage 1.

Nu afdelingsmanagers nadrukkelijk verantwoordelijkheid dragen voor de verwerkingen die op de afdeling worden verricht, is binnen elke afdeling een aanspreekpunt belast met de dagelijkse praktijk die samenhangt met de bevoegdheden en verantwoordelijkheden als genoemd in paragraaf 5.2. Daarnaast zal de rol van afdelingsmanager voor een deel bestaan uit het vertalen van het concernbeleid naar een specifiek afdelingsbeleid.

5.6 Externe relaties/verwerkersovereenkomst

Het verwerken van persoonsgegevens is geen doel op zich, maar zal steeds in het teken staan van een ander gerechtvaardigd doel dat met die verwerking zal worden bereikt (het verlenen van zorg, het houden van toezicht of het uitbetalen van salarissen). Ten behoeve van dat andere doel zullen vaak persoonsgegevens van elders betrokken worden of zullen persoonsgegevens worden overgedragen aan anderen.

Bij het verwerken van persoonsgegevens elders worden in de AVG twee mogelijke samenwerkingsconstructies genoemd; gezamenlijke verwerkingsverantwoordelijkheid en de verwerking namens de verwerkingsverantwoordelijke. Buiten deze twee in de AVG genoemde samenwerkingsconstructies is ook nog denkbaar dat de persoonsgegevens die door de gemeente Ede worden verwerkt worden overgedragen naar een andere verwerkingsverantwoordelijke (denk bij het sociaal domein aan een zorginstelling waarbij de overdracht aan de andere verwerkingsverantwoordelijke bij wet geregeld is).

A gezamenlijke verwerkingsverantwoordelijkheid

Van een gezamenlijk verwerkingsverantwoordelijkheid is sprake wanneer twee of meer verwerkingsverantwoordelijken gezamenlijk de doeleinden en middelen van de verwerking bepalen. In dat geval stellen zij op transparante wijze hun respectieve verantwoordelijkheden voor de nakoming van hun verplichting uit hoofde van de AVG vast, met name met betrekking tot de uitoefening van rechten van betrokkenen en het verstrekken van informatie aan hen. De relatie tussen de verwerkingsverantwoordelijken onderling wordt bestendigd door middel van een protocol.

B verwerkingsverantwoordelijke en verwerker

Wanneer een verwerking, namens een verwerkingsverantwoordelijke wordt verricht, en de verwerker geen zeggenschap heeft over doel en middel van de verwerking, dan doet de verwerkingsverantwoordelijke uitsluitend een beroep op verwerkers die afdoende garanties met betrekking tot het toepassen van passende technische en organisatorische maatregelen bieden opdat de verwerking voldoet aan de eisen van de AVG.

De gemeente Ede blijft als verwerkingsverantwoordelijke (mede-)aansprakelijk voor de geschonden rechten van betrokkenen door nalatigheden van de kant van de verwerker. Om de verantwoordelijkheid en aansprakelijkheden goed uit elkaar te houden zal de gemeente Ede in deze situaties gebruik maken van verwerkersovereenkomsten. Het gebruik van verwerkersovereenkomsten is een verplichting die voortvloeit uit de AVG. Als gemeente Ede hanteren we de model-verwerkersovereenkomst van de VNG.

C Overdracht van persoonsgegevens aan een andere verwerkingsverantwoordelijke

Daar waar het gaat om een overdracht van de persoonsgegevens (bijvoorbeeld in de vorm van bestanden) aan een andere verwerkingsverantwoordelijke zal er na overdracht geen gebondenheid meer zijn van de gemeente Ede. De inspanning van de gemeente Ede blijft hier beperkt tot het vaststellen of de ontvangende partij daadwerkelijk verwerkingsverantwoordelijke is. Dit speelt bijvoorbeeld in het geval van zorgaanbieders, waarbij de gemeente de toegang/toeleiding/indicering doet en een zorgaanbieder vervolgens de toegekende zorg aanbiedt.

6 Privacybeleid

In de AVG worden een aantal generieke normen gesteld waar de verwerkingsverantwoordelijke inhoud aan moet geven. Door het normenkader zelf vorm te geven kan de verwerkingsverantwoordelijke eigen accenten aanbrengen of beleidsuitgangspunten toevoegen. De gemeente Ede hecht er waarde aan dat de persoonsgegevens die aan haar zijn toevertrouwd alleen gebruikt worden voor de doeleinden waarvoor zij zijn gegeven. Dit wordt anders als de gegevensbescherming een gevaar oplevert voor hulpverlening en veiligheid. De gemeente zoekt in dergelijke gevallen de grenzen van de privacywetgeving op als daarmee een groter gevaar kan worden afgewend dat kan ontstaan als medewerkers en andere hulpverleners langs elkaar heen werken. Beslissingen die in dat verband genomen worden zullen duidelijk gemotiveerd worden.

Het beleid van de gemeente is ook gericht op transparantie en bewustwording. Zowel intern als extern zal er een open communicatie zijn over de wijze van verwerking van persoonsgegevens.

Binnen het thema beleid verdienen vier aspecten nadere invulling; rechten van betrokkenen, geautomatiseerde verwerkingen, datalekken en bewaren van persoonsgegevens.

6.1 Rechten van betrokkenen

Binnen de AVG worden verschillende rechten toegekend aan betrokkenen opdat zij steeds de regie kunnen voeren op de persoonsgegevens die bij de gemeente Ede worden verwerkt. Deze rechten staan in de artikelen 15 tot en met 22 van de AVG. Artikel 12 van de AVG bepaalt dat verwerkingsverantwoordelijke de uitoefening van de rechten van de betrokkene faciliteert.

Het uitgangspunt voor de gemeente Ede is dat gestreefd wordt naar een maximale transparantie tegenover de betrokkene waar het gaat om de 'eigen' persoonsgegevens. De gemeente Ede heeft een duidelijke ingang om privacyrechten uit te oefenen (e-formulier op de website of fysiek bij de balie Publiekszaken)

6.2 Geautomatiseerde verwerkingen

Onder geautomatiseerde verwerkingen wordt verstaan gebruikmaking van elektronische middelen om gegevens te verwerken. Een voorbeeld is profilering en algoritmen. Als de gemeente Ede hier gebruik van wil maken zal vooraf moeten worden bepaald of dit conform de AVG kan plaatsvinden en moet de verwerking worden opgenomen in het verwerkingsregister.

Voor onderzoeken zal de gemeente, indien dat in het kader van het onderzoek gewenst is, gebruik maken van Big data en tracking wanneer de aldus verzamelde gegevens niet te herleiden zijn tot een natuurlijke persoon. In die gevallen waarin de gemeente gebruik maakt van Big data onderzoeken en tracking, dan zal zij daarover vooraf informatie verstrekken op de gemeentelijke website. Data-analyse (zoals voor beleidsinformatie) is een onderwerp dat in opkomst is, ook bij de gemeente Ede. De gemeente Ede draagt er zorg voor dat dergelijk gebruik van data wordt afgewogen en conform de AVG plaatsvindt.

De gemeente maakt op dit moment gebruik van cameratoezicht. Dit zal in de toekomst niet anders worden. De gemeente zal, net als nu, op duidelijke wijze kenbaar maken wanneer iemand zich in het cameragebied bevindt.

6.3 Datalekken

Van een datalek is sprake bij een onrechtmatige verwerking en als persoonsgegevens in handen vallen van derden die geen toegang tot die gegevens zouden mogen hebben. Een datalek is het gevolg van een beveiligingsincident. In de meeste gevallen gaat het om uitgelekte computerbestanden, al kan een gestolen geprinte klantenlijst evengoed een datalek vormen. Andere voorbeelden: cyberaanvallen (incl. DDos), e-mail verzonden naar verkeerde adressen, gestolen laptops of bedrijfstelefoons, afgedankte niet-schoongemaakte computers en verloren usb-sticks.

Illegaal verkregen bedrijfsgegevens over een productieproces of marktstrategie betreffen kostbare informatie, maar vallen niet onder de gangbare definitie van datalek.

De gemeente Ede heeft een protocol rondom de meldplicht datalekken. Wanneer een (potentieel) datalek gemeld wordt beoordelen een aantal medewerkers, waaronder de CISO, of er sprake is van een datalek en of dit gemeld moet worden bij de AP en betrokkene(n).

6.4 Bewaren van persoonsgegevens

Persoonsgegevens mogen niet langer worden bewaard dan noodzakelijk is voor de verwerking. Voor wat betreft het bewaren van persoonsgegevens gelden voor de gemeente Ede twee regiem, het wettelijke regiem en het niet wettelijke regiem.

Voor sommige verwerkingen van persoonsgegevens geldt dat deze persoonsgegevens op grond van de Archiefwet of andere materiële wetten een minimale termijn bewaard moeten blijven. Een voorbeeld is het jeugdhulpdossier dat 15 jaar nadat de jeugdhulp beëindigd is bewaard moet blijven. De AVG gaat niet in op de wettelijke termijnen die bestaan of in de toekomst zullen ontstaan.

Voor die verwerkingen waarvoor geen wettelijke termijn bestaat geldt dat de verwerkte persoonsgegevens worden bewaard zo lang dit noodzakelijk is. De (wettelijke) bewaartermijn wordt bepaald en bij de verwerking vastgelegd in het verwerkingsregister.

7 Werkprocessen

In dit hoofdstuk staat de vraag centraal op welke wijze de gemeente Ede de verwerking van persoonsgegevens vorm geeft in bedrijfsprocessen en op welke wijze medewerkers gebruik kunnen maken van databases. In paragraaf 7.1 zal het kader geschetst worden hoe verwerking van persoonsgegevens in de bedrijfsprocessen moet worden ingebed. In paragraaf 7.2 wordt een bijzondere toepassing van verwerking van persoonsgegevens besproken waar hulpverleners en veiligheidsadviseurs mee te maken hebben in de dagelijks praktijk. Paragraaf 7.3 gaat dieper in op triages die hoofdzakelijk voorkomen in het sociaal domein. In de laatste paragraaf wordt besproken hoe met Data Protection Impact Assessments (DPIA's) privacyrisico's van gegevensverwerkingen in beeld gebracht worden en hoe maatregelen om privacyrisico's te beperken ingebed kunnen worden in de werkprocessen.

7.1 Inbedding in primaire processen

De AVG eist dat voor iedere verwerking van persoonsgegevens de beginselen inzake verwerking van persoonsgegevens in achtgenomen zijn. Deze beginselen vloeien voort uit artikel 5 en 6 AVG.

Zo moet de verwerking van persoonsgegevens kunnen steunen op welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Voor werkprocessen binnen de gemeente Ede betekent dit dat bij verwerkingen een geldige reden moet zijn om de inperking van het grondrecht privacy te rechtvaardigen. Ontbreekt een dergelijke reden, dan is de verwerking illegaal en zal zij moeten worden beëindigd.

Concreet betekent een en ander dat er zicht moet zijn op de taken van medewerkers waarbij persoonsgegevens worden verwerkt. Aan de hand van het overzicht van gegevensverwerkingen van de medewerkers zullen door het afdelingsmanagement gerechtvaardigde doeleinden moeten worden geformuleerd om de verwerking voort te kunnen zetten. Nadat doeleinden zijn geformuleerd is het noodzakelijk om te beoordelen welke persoonsgegevens ten minste verwerkt moeten worden om dat doel te kunnen bereiken. Persoonsgegevens die bovenmatig zijn kunnen buiten de verwerking blijven.

De volgende stap is dat aansluiting gevonden wordt bij een van de grondslagen uit artikel 6 AVG (zie tevens paragraaf 4.4). Voor de gemeente Ede zal gaan gelden dat veel verwerkingen als grondslag de goede vervulling van een publieke taak kennen. In bijzondere gevallen zal een beroep op een van de andere grondslagen mogelijk of, in geval van toestemming, nodig zijn.

7.2 Verwerkingsregister

Zoals in het hoofdstuk Governance is aangegeven ligt de ambtelijke verantwoordelijkheid voor het verwerken van persoonsgegevens bij de afdelingsmanager. Zij brengen in beeld en bewaken het overzicht van de gegevensverwerkingen die op de afdeling plaatsvinden. Een verwerking wordt beschreven aan de hand van een formulier en vervolgens opgenomen in het verwerkingsregister.

Kader van het overzicht wordt gevormd door de AVG. Zo zal onder meer vastgesteld moeten zijn dat de verwerking een gerechtvaardigd doel kent en gebaseerd is op een rechtmatige grondslag.

De juridisch privacy adviseur en de FG beheren het verwerkingsregister. Mutaties worden gemeld door de ambtelijke verantwoordelijke.

7.3 Triage

Aparte aandacht wordt gegeven aan het proces rond de triage. Triage speelt op casusniveau en vraagt van de medewerker om een professionele inschatting te maken wat de ernst van de problematiek is en welke verwerking van persoonsgegevens daarbij wenselijk is. Met name bij een multi-probleemsituaties in het sociaal domein kan er opschaling nodig zijn waardoor meer persoonsgegevens worden verwerkt of persoonsgegevens met anderen worden gedeeld. Dit is te rechtvaardigen om te voorkomen dat privacy in de weg gaat staan aan een effectieve hulpverlening.

Medewerkers bepalen per casus het doel waarvoor de gegevensverwerking noodzakelijk is. Daarnaast bepalen zij of er niet bovenmatig gegevens worden verwerkt of dat gegevens niet op een andere, minder ingrijpende wijze, kunnen worden verwerkt. Van belang is dat deze afweging door de medewerker wordt vastgelegd. Triage momenten worden benoemd in het werkproces. De grondslag voor triage is voor de gemeente Ede het algemeen belang/openbaar gezag. Dit betekent concreet dat het toepassen van triage beperkt is tot die werkprocessen waarbij het uitwisselen van persoonsgegevens binnen en buiten de eigen organisatie terug te voeren is op een wettelijke bevoegdheid/taak.

7.4 Data Protection Impact Assessment (gegevensbeschermingseffectbeoordeling)

Met het uitvoeren van een Data Protection Impact Assessment (DPIA) wordt inzicht verkregen in de privacyrisico's van een nieuwe dienst of een nieuw product. Maar ook het hergebruik van reeds verwerkte data voor nieuwe toepassingen is een voorbeeld waarvoor een DPIA een duidelijk inzicht geeft aan de betrokken risico's.

Een DPIA wordt bij voorkeur in een zo vroeg mogelijk stadium van het ontwerpproces uitgevoerd, zodat uitkomsten van de PIA nog meegenomen kunnen worden en invulling gegeven kan worden aan 'privacy by

design'. Een DPIA kan ook in een later stadium uitgevoerd worden, omdat de meeste processen 'doorontwikkeld' worden en ook later nog privacyrisico's kunnen worden ingedamd.

Het is niet noodzakelijk om voor alle processen waarbij persoonsgegevens worden verwerkt een DPIA uit te voeren. Voor een aantal onderwerpen is een DPIA verplicht, de gemeente Ede beschikt over een vragenlijst aan de hand waarvan kan worden bepaald of een DPIA verplicht is of niet.

DPIA's kunnen worden begeleid door medewerkers van IPPM en de juridisch privacy-adviseur

Medewerkers van IPPM zullen over het algemeen als initiator optreden en beslissen voor welke verwerkingen een DPIA wordt uitgevoerd. De afdelingsmanager blijft verantwoordelijk voor de keuze voor welke verwerkingen een DPIA wordt uitgevoerd en voor het uitvoeren van de maatregelen die (mogelijk) uit de DPIA voortvloeien.

Tijdens de uitvoering van een DPIA wordt aan de hand van een lijst met vragen bepaald of er sprake is van (hoge) privacyrisico's en worden maatregelen vastgesteld die deze risico's zoveel mogelijk beperken.

8 Bewustwording

8.1 Privacyveilig werken

Het is belangrijk dat privacy niet alleen leeft bij een aantal 'ingewijden', maar breed uitgedragen wordt binnen de organisatie. Dit vraagt om een interne bewustwording hoe omgegaan moet worden met de belangen van personen die persoonsgegevens aan de gemeente Ede hebben toevertrouwd.

Om bewust te blijven van de risico's en de schade die kan ontstaan door gegevensbescherming niet serieus te nemen is een continue communicatie met betrekking tot dit onderwerp nodig. Binnen de kaders van de gemeente Ede wordt op twee niveaus invulling gegeven aan het bewustwordingsproces; op concern- en op afdelingsniveau.

8.2 Bewustwording door concernactiviteiten

Binnen concerncontrol is de onafhankelijke positie van FG belegd. Tot de taken van de FG behoort in ieder geval informeren en adviseren van de verwerkingsverantwoordelijke en de verwerker over hun verplichtingen vanuit de AVG.

Door kritisch na te denken over alle aspecten die samenhangen met de verwerking, zoals omvang en doel van de verwerking of de technische infrastructuur krijgen medewerkers inzicht in de kaders die gesteld worden aan een goede bescherming van persoonsgegevens.

Dit beleidsplan vormt een bron voor communicatie naar de afdelingen. Afdelingen zijn gehouden om hun taken en verantwoordelijkheden met betrekking tot privacy & informatieveiligheid uit te voeren. In de eerste helft van 2018 is de verantwoordelijkheid voor de verwerkingen in het register en voor privacy-acties naar aanleiding van dit beleidsplan overgedragen aan de afdelingsmanagers. Een- tot tweejaarlijks worden zij hieraan herinnerd.

Naast deze activiteiten kennen we een concernbreed bewustwordingsplan waar jaarlijks uitvoering aan wordt gegeven door de privacy-driehoek.

8.3 Bewustwording door afdelingsactiviteiten

Uitgangspunt van bewustwording op afdelingsniveau is om het bewustwordingsproces zo dicht mogelijk bij de medewerkers te organiseren. Welke communicatiemiddelen en trainingen worden ingezet ligt bij het afdelingsmanagement. De rol van de driehoek is ondersteunend.

In de bedrijfsvoeringsgesprekken wordt besproken of opvolging is gegeven aan het onderwerp bewustwording.

9 Beheer en opslag van persoonsgegevens

9.1 Opslag van persoonsgegevens

Persoonsgegevens worden binnen de gemeente Ede (vrijwel) altijd digitaal opgeslagen. Voor opslag van gegevens beschikt de gemeente Ede over een eigen, afgeschermd netwerk. De manier waarop Ede haar netwerk en gegevens beveiligd is in overeenstemming met de gemeentelijke beveiligingsnormen (BIO, zie ook 4.6)

Opslag gebeurt op de volgende manieren:

- In centrale databases die door verschillende gebruikers te benaderen en te bewerken zijn. Alle grote registraties van persoonsgegevens zijn Ede zijn opgenomen in centrale databases.
- Binnen decentrale databases en spreadsheets die middels algemene kantoorautomatiseringssoftware te benaderen zijn. Dit betreft kleinschalige registraties met een zeer specifiek doel.
- Op ongestructureerde basis: in documenten, afbeeldingen, mailapplicatie en dergelijke. Dit betreft geen registraties maar specifieke persoonsgegevens over een of enkele personen.

Voor de opslag van persoonsgegevens gelden de volgende uitgangspunten:

- Opslag in centrale databases heeft sterk de voorkeur boven decentrale opslag. Centrale databases kennen een hogere beschikbaarheid, daarnaast is de integriteit en de vertrouwelijkheid van de data veel beter te waarborgen.
- Opslag van persoonsgegevens geschied op het goed beveiligde netwerk van de gemeente Ede.
- Lokale opslag zoals smartphones en laptops worden afdoende versleuteld.

De gemeente Ede kent diverse voorzieningen om de beschikbaarheid van de persoonsgegevens te waarborgen. Vitale ICT-systemen en componenten zijn dubbel uitgevoerd, en alle gegevens op het interne netwerk worden dagelijks geback-up't. Ook deze maatregelen zijn in lijn met de gemeentelijke beveiligingsnormen.

9.2 Toegang tot en beheer van persoonsgegevens

Alleen geautoriseerde personen hebben toegang tot het netwerk van Ede en daarmee tot persoonsgegevens. Deze toegang tot het netwerk is beperkt tot applicaties en bestanden die vanuit de functie van de betrokkene noodzakelijk zijn. Voor toegang tot gestructureerde persoonsgegevens in centrale databases geldt een fijnmaziger toegang tot op specifiek gegevensniveau. Dit gebeurt op basis van rollen waarbij per medewerker of per functie een of meerdere rollen worden toegekend. Achter deze rollen hangt een autorisatieschema waarbij per type persoonsgegeven is vastgelegd in hoeverre deze vanuit de rol ingezien en veranderd mag worden. De toewijzing van rollen aan medewerkers wordt vastgelegd in autorisatiematrices en periodiek gecontroleerd.

De benodigde toegangsrechten worden vastgesteld door het lijnmanagement. Zij zijn verantwoordelijk voor de verwerking van persoonsgegevens (zie ook paragraaf 5.2) het beheer van de daarvoor benodigde applicaties en voor het treffen van afdoende beveiligingsmaatregelen. Het beheer van applicaties, en de daarin opgenomen persoonsgegevens en het daadwerkelijk toewijzen en inrichten van de toegangsrechten wordt uitgevoerd door applicatiebeheerders. De gemeente heeft hier een formele procedure voor. Toegang tot persoonsgegevens wordt op gegevens- en medewerkersniveau geregistreerd (gelogd). Op deze manier is te achterhalen wie op welk tijdstip welke gegevens heeft geraadpleegd. Ede kent procedures om deze logging te gebruiken bij privacyincidenten.

Overzicht taken en verantwoordelijkheden

De Functionaris Gegevensbescherming (FG)

De functionaris voor de gegevensbescherming (FG, ook wel Data Protection Officer (DPO) genoemd), is de (wettelijke) interne toezichthouder op de verwerking van persoonsgegevens binnen de organisatie. De FG houdt binnen de organisatie toezicht op de toepassing en naleving van de privacywetgeving. De wettelijke taken en bevoegdheden van de FG geven deze functionaris een onafhankelijke positie in de organisatie.

De FG heeft in ieder geval de volgende taken en verantwoordelijkheden:

- Informeren en adviseren van de gemeente over hun verplichtingen volgens de AVG ;
- Toezien op naleving van AVG en andere EU wet- en regelgeving en nationale bepalingen omtrent gegevensbescherming;
- Toezien op naleving van het gemeentelijke beleid met betrekking tot de verwerking van persoonsgegevens;
- Eerste aanspreekpunt voor de Autoriteit Persoonsgegevens (AP) en kan afstemmen met de AP;
- Toezien op toewijzing van verantwoordelijkheden, bewustmaking en opleiding van medewerkers;
- Adviseren met betrekking tot vraagstukken over de verwerking van persoonsgegevens;
- Adviseren met betrekking tot veiligheidsincidenten met persoonsgegevens;
- Adviseren met betrekking tot de DPIA en het toezien of de uitvoering daarvan in overeenstemming is met de AVG;
- Toezien op en adviseren over de afhandeling van vragen en klachten over het gebruik van persoonsgegevens;
- Adviseren en ondersteunen bij het opstellen van privacynormen, procedure-, -beleid, -regelingen of – gedragscodes;
- Rechtstreeks aan het college van b&w rapporteren.

De privacy-adviseur/privacy-officer

Deze rol is gericht op de uitvoering en de naleving van de privacy wetgeving. De privacy-adviseur adviseert over privacybescherming en over activiteiten ter bescherming van persoonsgegevens.

De privacy-adviseur heeft in ieder geval de volgende taken:

- Het beoordelen van de verwerking van persoonsgegevens tegen de achtergrond van de kaders van de (Europese)privacywetgeving. Adviseren bij wijzigingen in procesuitvoering en bedrijfsvoering en de toepassing van een privacy impact assessment (DPIA).
- Adviseren bij programma's en projecten waarvan het resultaat gevolgen kan hebben voor de wijze van verwerking van persoonsgegevens.
- Adviseren over verwerkersovereenkomsten en privacybepalingen in overige documenten;
- Coördineren van verzoeken over verwerking van persoonsgegevens (zogenaamde AVG-verzoeken/verzoeken m.b.t. de rechten van betrokkenen) en concernbrede verzoeken behandelen;
- Zorgen voor processen voor de behandeling van AVG-verzoeken, DPIA en register van verwerkingsactiviteiten;
- Bijdragen aan privacybewustzijn;
- Adviseren met betrekking tot vraagstukken over de verwerking van persoonsgegevens;
- Beheren van het privacybeleid;
- Beheer en onderhoud van de standaarddocumenten voor verwerkersovereenkomsten, convenanten en reglementen;
- Advisering en ondersteuning bij het besluitvormingsproces en het afsluiten van verwerkersovereenkomsten, convenanten en de vaststelling van reglementen.

Chief Information Security Officer (CISO)

Deze rol is op organisatieniveau verantwoordelijk voor het actueel houden van het informatieveiligheidsbeleid, het coördineren van de uitvoering van het beleid, het adviseren bij projecten, het beheersen van risico's, evenals het opstellen van rapportages. De CISO heeft in ieder geval de volgende verantwoordelijkheden:

- Richt procedures in voor het afhandelen van datalekken en draagt zorg voor de afhandeling van ingekomen veiligheidsincidenten;
- Stelt de informatieveiligheidsanalyse op en zorgt voor de actualisatie hiervan;
- Coördineert de prioritering van informatieveiligheidsmaatregelen uit de informatieveiligheidsanalyse en de uitvoering van het actieplan informatieveiligheid;

- Ondersteunt de directie en de afdelingsmanagers met kennis over informatieveiligheid en privacy, zodat zij hun verantwoordelijkheid voor de betrouwbaarheid en vertrouwelijkheid van de informatievoorziening juist kunnen invullen;
- Is aanspreekpunt voor medewerkers van de gemeente over het onderwerp informatieveiligheid;
- Volgt de externe invloeden die van invloed zijn op beleid;
- bevordert het veiligheids- en privacybewustzijn in de organisatie;
- Houdt de registratie van informatieveiligheidsincidenten bij in een incidentenregister en is verantwoordelijk voor de juiste afhandeling en evaluatie van incidenten.
- Implementeren en beheren BIO

Afdelingen

De afdelingsmanagers zijn primair verantwoordelijk voor de verwerking van persoonsgegevens in de processen op hun afdeling. Als zodanig is de afdelingsmanager eigenaar van deze persoonsgegevens.

De eigenaar heeft in ieder geval de volgende taken en verantwoordelijkheden:

- Actueel houden van de verwerkingen zoals deze zijn opgenomen in het register van verwerkingsactiviteiten;
- Nieuwe verwerkingen melden bij de privacy-adviseur;
- Behandelen van verzoeken over privacyrechten (zogenaamde AVG-verzoeken/verzoeken m.b.t. de rechten van betrokkenen);
- Aanwijzen privacy-ambassadeur;
- Bij een nieuwe verwerking of wijziging binnen een bestaande verwerking toetsen of een Data Protection Impact Assessment (DPIA) verplicht is, uitvoeren DPIA en opvolging geven aan de resultaten van de DPIA;
- Afsluiten, beheren en actualiseren verwerkersovereenkomsten;
- Het belang van informatieveiligheid en privacy (periodiek) onder de aandacht brengen van de afdeling;
- Uitvoeren van het beleid ten aanzien van de verwerking van persoonsgegevens die onder zijn of haar verantwoordelijkheid vallen;
- Archivering;
- Melden incidenten met betrekking tot de veiligheid van informatie en/of persoonsgegevens.