GEMEENTE LOPIK

GEMEENTEBLAD

Officiële uitgave van de gemeente Lopik

Nr. 46119

30 januari 2024

Tactisch Privacybeleid Gemeente Lopik 2023-2026

Het college van burgemeester en wethouders van de gemeente Lopik,

gezien het advies van de afdeling Bedrijfsvoering van 13 december 2023;

besluit:

Het Strategisch InformatieBeveiligings- en Privacybeleid en het Tactisch Privacybeleid voor de periode 2023 – 2026 vaststellen.

Tactisch Privacybeleid Gemeente Lopik 2023-2026

1. Inleiding

Dit beleidsdocument op tactisch niveau is een aanvulling op het strategisch InformatieBeveiligings- en Privacybeleid (IBP-beleid) van de gemeente Lopik. Het is afgeleid van het "Beleidsplan veilig omgaan met persoonsgegevens in de gemeente Lopik", geschreven door H. Vegter in 2018. Het nieuwe IBP-beleid bevat slechts de hoofdlijnen waarop het privacybeleid wordt vormgegeven. Dit tactische privacybeleid werkt deze hoofdlijnen verder uit.

1.1 Leeswijzer

In hoofdstuk 2 wordt het begrip privacy besproken als uitwerking van de Algemene Verordening Gegevensbescherming (AVG). Hoofdstuk 3 beschrijft vervolgens hoe de taken en verantwoordelijkheden in de organisatie belegd zijn. Hoofdstuk 4 gaat over de inrichting van de werkprocessen op het aspect privacy.

2. Privacy

2.1 Begrippen

In dit document worden verschillende begrippen gehanteerd vanuit de privacywetgeving. 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 identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon;
- 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;
- Verwerkersovereenkomst: een vormvrije overeenkomst die gesloten wordt tussen eindeverantwoordelijke en verwerker en waarbij de verantwoordelijke het doel en het middel van de verwerking bepaalt;
- Bestand: elk gestructureerd geheel van persoonsgegevens die volgens bepaalde criteria toegankelijk zijn, ongeacht of dit geheel gecentraliseerd of gedecentraliseerd is dan wel op functionele of geografische gronden is verspreid;

- 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.

2.2 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.

2.2.1 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 worden geformuleerd. Uitgangspunt van de verordening is dat persoonsgegevens voor een welbepaald, uitdrukkelijk omschreven en gerechtvaardigd doel worden verzameld. Het is een simpele aanpak om per team te laten vaststellen voor welke doelen persoonsgegevens worden verwerkt. Hierbij kan worden gedacht aan vergunningverlening, subsidievaststelling of het bepalen van een uitkering. Deze doeleinden worden opgenomen in het register van verwerkingen. In de praktijk wordt het toegestaan dat een doelomschrijving uit meerdere onderdelen bestaat, bijvoorbeeld in een constructie hoofddoel en subdoelen of nevendoelen. Van belang daarbij is dat deze doelstellingen onderling verenigbaar zijn. Het is ook mogelijk dat verwerkingen na melding voor andere doeleinden worden aangewend. Ook dit laatste is toegestaan, mits dit latere doel verenigbaar is met het oorspronkelijke.

Wanneer de doelen per team zijn bepaald, moet worden beoordeeld wat het takenpakket is van de medewerkers. Aan de hand van het takenpakket wordt beoordeeld welke persoonsgegevens daarvoor moeten worden verwerkt. Voor verwerkingen die in omvang (men verwerkt gegevens van grotere groepen personen) of soort (men verwerkt meer gegevens dan noodzakelijk) niet noodzakelijk zijn voor de uitvoering van taken, kan gesteld worden dat hier geen te rechtvaardigen doel mee wordt gediend. Deze verwerkingen moeten om die reden worden beëindigd.

2.2.2 Toereikend, ter zake dienend en niet bovenmatig
Voor al deze afzonderlijke doelen dient vervolgens te worden vastgesteld welke persoonsgegevens hiertoe noodzakelijkerwijs wel 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 ontstaat. Ter verduidelijking; een winkelier, die een registratie bijhoudt van wanbetalers, doet een ontoereikende verwerking als hij niet ook 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 worden aangewend om het koopgedrag te analyseren. Tot

slot hangt bovenmatig ook samen met het doel. Houdt de winkelier een registratie bij van wanbetalers voor zijn administratie, dan is het registeren van de waarde niet bovenmatig. Het bijhouden van het aantal goederen is dat mogelijk wel.

Op teamniveau moet per verwerking worden vastgesteld welke persoonsgegevens ten minste noodzakelijk zijn om het doel te kunnen bereiken.

2.2.3 Vereisten van doelmatigheid, proportionaliteit en subsidiariteit

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 het recht op privacy van de betrokkene Op grond van 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 verwerkt (bijvoorbeeld het verkrijgen van de informatie uit open data).

Ook hier moet per team worden beoordeeld of de verwerking doelmatig is, de inbreuk op de persoonlijke levenssfeer niet zwaarder weegt dan de verwerking en of de persoonsgegevens ook op een minder ingrijpende wijze verkregen kunnen worden.

2.2.4 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:

- Ondubbelzinnige toestemming.
- Ter uitvoering van een overeenkomst.
- Ter uitvoering van een wettelijke taak.
- Ter vrijwaring van een vitaal belang.
- Voor een goede vervulling van een publieke taak of van een taak in het kader van uitoefening openbaar gezag opgedragen aan de verwerkingsverantwoordelijke of vanuit gerechtvaardigde belangen.

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 eerste grondslag alleen gebruikt wordt (ondubbelzinnige toestemming) als op grond van een van de andere grondslagen geen persoonsgegevens kunnen worden verwerkt. Als op basis van een andere grondslag (voor de gemeente Lopik is dit in de regel het uitvoeren van wettelijke taken of een goede vervulling van publieke taken) het mogelijk is gegevens te verzamelen, dan wordt geen toestemming aan de betrokkene gevraagd, tenzij een wettelijke bepaling daartoe verplicht.

2.2.5 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 Lopik 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 bepaald door wet- en regelgeving of door de verwerkingsverantwoordelijke. Om te zorgen dat de verwerker zich houdt aan de instructies van de verwerkingsverantwoordelijke en kan garanderen aan de verwerkingsverantwoordelijke dat hij 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 overeenkomst tot opdracht of samenwerkingsovereenkomst. Het verstandigst is echter om de verwerkingsovereenkomst op te hangen aan de mantelovereenkomst. Zo wordt strijdigheid tussen verschillende overeenkomsten voorkomen. Het template van de verwerkersovereenkomst is als bijlage 1 aan dit privacybeleid toegevoegd.

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 in termen van overdrachtsmoment en verdeling van de aansprakelijkheden.
Voor de gemeente Lopik geldt dat, als sprake is van een gezamenlijke verwerkingsverantwoordelijkheid, dit vooraf is vastgelegd in een samenwerkingsovereenkomst, aangevuld met het protocol gegevensbescherming (zie bijlage 2). Een voorbeeld waarbij persoonsgegevens van de ene verantwoordelijke naar de andere verantwoordelijke worden overgedragen is te vinden in Hoofdstuk 5 van de Wet maatschappelijke ondersteuning waar zorginstellingen als zelfstandig verantwoordelijke worden genoemd.

2.2.6 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 Lopik wordt aan deze eis van passende maatregelen invulling gegeven door het invoeren van de maatregelenset van de Baseline Informatiebeveiliging Overheid (BIO). 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 passend 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 boven op het basisbeveiligingsniveau.
- Het invoeren van een proces van plannen, uitvoeren, toetsen en bijsturen (PDCA) waarbij de maatregelenset systematisch gecontroleerd wordt op effectiviteit en zo nodig aangepast wordt om het passende beveiligingsniveau blijvend te kunnen waarborgen.

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

2.3 Rechten van betrokkenen

Binnen de AVG worden verschillende rechten toegekend aan betrokkenen zodat zij steeds de regie kunnen voeren op de persoonsgegevens die bij de gemeente Lopik worden verwerkt. Het gaat om de volgende rechten:

1. Recht op informatie (artikel 12 AVG)
Er dienen maatregelen te worden genomen zodat de betrokkene op een beknopte, transparante, begrijpelijke en in gemakkelijk toegankelijke vorm informatie kan verkrijgen over zijn persoonsgegevens en geïnformeerd wordt over verwerkingsactiviteiten.

2. Recht op inzage (artikel 15 AVG)
Betrokkene heeft het recht uitsluitsel te krijgen over het al dan niet verwerken van hem betreffende persoonsgegevens en om inzage te verkrijgen van die persoonsgegevens en de volgende informatie:

- Verwerkingsdoelen.
- Betrokken categorieën van persoonsgegevens.
- Ontvangers of categorieën ontvangers aan wie persoonsgegevens worden verstrekt.
- Duur van de verwerking en opslag.
- Informatie over de bron van de gegevens (indien gegevens niet bij betrokkene worden verzameld).
- Het bestaan van geautomatiseerde besluitvorming, het belang en de te verwachten gevolgen voor betrokkene.

3. Recht op rectificatie (artikel 16 AVG en 19 AVG)
Betrokkene heeft het recht dat onjuiste persoonsgegevens onverwijld worden gerectificeerd en dat onvolledige gegevens worden aangevuld. De verwerkingsverantwoordelijke stelt iedere ontvanger op de hoogte van de rectificatie of aanvulling.

4. Recht op gegevenswissing (artikel 17 AVG en 19 AVG)
Onder omstandigheden heeft betrokkene het recht dat zijn gegevens zonder onredelijke vertraging worden gewist. Per verwerking moet worden bepaald of gegevenswissing mogelijk is.

5. Recht op beperking van de verwerking (artikel 18 AVG)

Onder omstandigheden heeft betrokkene het recht om een beperking van de verwerking te verkrijgen, indien de juistheid van de persoonsgegevens worden betwist, de verwerking onrechtmatig is, de persoonsgegevens niet meer noodzakelijk zijn voor het doel waarvoor ze zijn verwerkt of indien betrokkenen bezwaar heeft gemaakt tegen de verwerking.

6. Recht op overdraagbaarheid (artikel 20 AVG)
Betrokkene heeft het recht om zijn persoonsgegevens in een gestructureerde, gangbare en machineleesbare vorm te verkrijgen en het recht deze gegevens over te dragen aan een andere verwerkingsverantwoordelijke.

7. Recht op bezwaar (artikel 21 AVG)
Betrokkene heeft steeds het recht bezwaar te maken tegen de verwerking. De verwerkingsverantwoordelijke staakt de verwerking, tenzij er dwingende gerechtvaardigde gronden zijn die zwaarder wegen dan de belangen van de betrokkene.

8. Recht om niet onderworpen te worden aan een enkel op geautomatiseerde verwerking gebaseerd besluit (artikel 22 AVG).
Betrokkene heeft het recht om niet onderworpen te worden aan een enkel op geautomatiseerde verwerking, waaronder profilering, gebaseerd besluit waaraan voor hem rechtsgevolgen zijn verbonden of dat hem anderszins in aanmerkelijke mate treft.

9. Klachtrecht en schadevergoedingsrecht (artikel 77 AVG en artikel 82 AVG)
Betrokkene heeft het recht een klacht in te dienen bij de toezichthoudende autoriteit en het recht op een vergoeding van materiële of immateriële schade ten gevolge van inbreuk op bepalingen AVG en waarvoor de verwerkingsverantwoordelijke aansprakelijk is jegens de betrokkene.

Het uitgangspunt voor de gemeente Lopik is dat wordt gestreefd naar een maximale transparantie tegenover de betrokkene waar het gaat om de ‘eigen’ persoonsgegevens.
Waar het gaat om het recht op informatie wijzen de gemeenten betrokkenen in algemeenheid op de website en in de correspondentie op het feit dat persoonsgegevens worden verwerkt en dat betrokkenen een aantal rechten hebben op grond van de AVG. Inhoudelijk worden deze verzoeken en bezwaren door de coördinator rechtsbescherming (zie paragraaf 3.4) begeleid.

2.4 Rechten personeelsleden
In het licht van de AVG zijn de gegevens van medewerkers eveneens gegevens van betrokkenen en verdienen om die reden aandacht.

De komst van de AVG biedt ook een goede gelegenheid om de verwerking van persoonsgegevens van medewerkers van de gemeente eens tegen het licht te houden. Er zijn twee situaties waarbij persoonsgegevens van medewerkers kunnen worden geopenbaard: via raads- en collegebesluiten of via persoonlijke correspondentie.

Voor raads- en collegestukken geldt dat deze stukken na besluitvorming op internet worden geplaatst. Op deze manier kan iedereen zien welke medewerker de auteur is geweest van het stuk. De vraag die voorligt is in hoeverre het zinvol is om de naam van medewerkers langs deze weg te openbaren? Al snel zal blijken dat er geen goede reden is te verzinnen waarom openbaar maken wenselijk is. Immers, medewerkers staan hoofdzakelijk (zo niet uitsluitend) ten dienste van het college van burgemeester en wethouders. In dat verband is het te billijken dat het college de naam van de behandelend ambtenaar te zien krijgt. Naderhand kan de naam door anonimisering worden verwijderd. De verantwoordelijk wethouder of burgemeester (die juist een publieke functie hebben) worden vervolgens wel genoemd bij het desbetreffende stuk dat op internet wordt geplaatst.

Bij raadsstukken worden evenmin namen van medewerkers vermeld. Het collegestuk wordt aan de raad aangeboden door de betreffende wethouder of de burgemeester.

In correspondentie naar burgers kunnen persoonsgegevens van de medewerker worden genoemd, indien dit noodzakelijk is (bijvoorbeeld welke Wmo-consulent een dossier gaat behandelen). In die gevallen dat er geen noodzaak is persoonsgegevens van medewerkers te delen, wordt de naam van de medewerker vervangen door een alias (bijvoorbeeld eerste letter voornaam en de eerste drie letters achternaam). De medewerker kan zelf deze keuze maken.

In geval sprake is van Woo-verzoeken kunnen de namen van medewerkers achterwege blijven. Uit artikel 10, eerste lid onder de Woo vloeit dit al voort. In het kader van dit privacybeleids wordt het artikel uit voornoemde regel gevolgd met de aanvulling dat er snel sprake is van een aantasting van de persoonlijke levenssfeer. Voor degene die Woo-verzoeken afhandelt, betekent dit een extra alertheid.

2.5 Geautomatiseerde verwerkingen van audio-opnamen en cameratoezicht
Onder geautomatiseerde verwerkingen wordt verstaan het met gebruikmaking van elektronische middelen verwerken van (persoons)gegevens. Een voorbeeld daarvan is profilering. Door het bezoeken van bepaalde gemeentelijke websites door betrokkenen kunnen bepaalde persoonlijke voorkeuren worden vastgelegd en geanalyseerd en kan de gemeente aan de bezoeker bepaalde gerichte producten of diensten aanbieden. Door de gemeente Lopik wordt hier geen gebruik van gemaakt.

Voor onderzoeken maakt de gemeente, indien dat in het kader van het onderzoek gewenst is, gebruik van Big data en tracking wanneer de verzamelde gegevens niet te herleiden zijn tot een natuurlijke persoon. In die gevallen waarin de gemeente gebruik maakt van Big data onderzoeken en tracking, verstrekt zij daarover vooraf informatie op de gemeentelijke website.

De gemeente Lopik maakt op dit moment gebruik van cameratoezicht op de gemeentewerf. Waar het gaat om cameratoezicht houdt de gemeente vast aan het standpunt van de Autoriteit Persoonsgegevens. Dit betekent dat minder vergaande maatregelen onvoldoende zijn gebleken, cameratoezicht plaatsvindt in samenhang met andere maatregelen, mensen worden geïnformeerd, camerabeelden worden niet langer dan 4 weken bewaard en er wordt een Data Protection Impact Assessment (DPIA) uitgevoerd.

De gemeente Lopik maakt gebruik van audio-opnamen in de raadszaal. Dit gebruik is toegestaan mits duidelijk wordt aangegeven aan betrokkenen dat audio-opnamen worden gemaakt.

2.6 Datalekken
Van een datalek is sprake bij een onrechtmatige verwerking en wanneer 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 verloren uitgeprinte klantenlijst evengoed een datalek vormen. Andere voorbeelden zijn: cyberaanvallen (incl. DDos), e-mail verzonden naar verkeerde adressen, onderschepte e-mails, niet-aangekomen post, gestolen laptops of bedrijfstelefoons, afgedankte niet-schoongemaakte computers en verloren usb-sticks.

Incidenten worden gemeld door medewerkers of verwerkers bij de helpdesk van de gemeente. In geval van een beveiligingsincident wordt de melding doorgezet naar de CISO, FG en PO. Zij analyseren de melding en bepalen of het beveiligingslek mogelijk ook een datalek is. Bij een vermoeden van een datalek zal de FG deze verder afhandelen conform de "Procedure afhandeling incidenten".

2.7 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 Lopik twee regimes: het wettelijke regime en het niet wettelijke regime. Uitgangspunt in de AVG is dat persoonsgegevens niet langer worden bewaard dan noodzakelijk voor het doel waarvoor het bestand is aangelegd.
Voor sommige verwerkingen van persoonsgegevens geldt dat persoonsgegevens op grond van de Archiefwet of andere materiële wetten een minimale termijn moeten blijven bewaard moeten.
Een voorbeeld is het jeugdhulpdossier dat 15 jaar nadat de jeugdhulp is beëindigd, bewaard moet blijven. Voor bouwdossiers geldt een algemene termijn van 20 jaar. Na 20 jaar worden de informatieve elementen uit het bouwdossier overgedragen aan het Nationaal Archief. Het moge duidelijk zijn dat als er een termijn geldt in een bijzondere wet, deze termijn prevaleert boven het algemene uitgangspunt van de AVG.

Voor wat betreft het archiveren van persoonsgegevens zoekt de gemeente Lopik aansluiting bij artikel 89 AVG. Archiveren in het algemeen belang is mogelijk, mits passende maatregelen zijn getroffen om de betrokkenen te beschermen. Vaststaat dat persoonsgegevens die voor een gerechtvaardigd doel zijn verwerkt, ook mogen worden verwerkt in de zin van archivering. Wel moet opnieuw worden beoordeeld of verdere dataminimalisatie mogelijk is. Is dataminimalisatie mogelijk door ontkoppeling van de persoonsgegevens met de overige gegevens, dan wordt daar voor gekozen. Als tussenvorm is het mogelijk om in het kader van archivering te werken met pseudoniemen.

Om archivering in goede banen te leiden, wordt er apart onderzoek gedaan naar het opslaan van persoonsgegevens in gemeentelijke archieven. De insteek is om vanuit het register van verwerkingen die bestanden te selecteren waarbij een afwijkend archiefregiem geldt en hiervoor separaat instructies te maken.

3. Organisatie, taken & verantwoordelijkheden

Om te voldoen aan de AVG zijn op bestuurlijk en ambtelijk niveau binnen de gemeente Lopik een aantal organisatorische maatregelen noodzakelijk. In paragraaf 3.1 en paragraaf 3.2 wordt de verdeling van bevoegdheden en verantwoordelijkheden geregeld tussen het bestuurlijke en ambtelijke niveau. Vanaf paragraaf 3.3 worden de functies benoemd die betrokken zijn bij het 'in control' brengen en houden van de gemeente Lopik.

3.1 Privacy op bestuurlijk niveau

Binnen de kaders van de AVG is het college bestuurlijk eindverantwoordelijke voor de verwerking van persoonsgegevens. Deze gezamenlijke verantwoordelijkheid wordt door de gemeente Lopik belegd bij een van de portefeuillehouders die als vast aanspreekpunt fungeert voor privacy-issues.
Op bestuurlijk niveau blijft dan alleen nog een afzonderlijke verantwoordelijkheid over voor de gemeenteraad voor de verwerkingen waarvoor zij eindverantwoordelijke is.

Het college wil optimaal gebruik maken van de ruimte die de AVG biedt om persoonsgegevens te verwerken. De AVG stelt als ondergrens dat de overheidsinstantie compliant moet zijn en passende technische en organisatorische maatregelen dient te nemen.
Er bestaat dus beleidsvrijheid. Deze beleidsvrijheid wordt primair op teamniveau ingevuld. Onder omstandigheden kan het college uitdrukkelijk worden gevraagd in te stemmen met een verwerking. Het afwegingskader daarbij is de bescherming van de privacy van de burger afgezet tegen een eigen belang van de gemeente, bijvoorbeeld de 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 worden persoonsgegevens zoveel mogelijk buiten collegebesluiten gehouden, tenzij de betrokkene toestemming heeft gegeven. Slechts in uitzonderlijke gevallen mogen persoonsgegevens zonder toestemming openbaar worden gemaakt.

Mocht het toch noodzakelijk zijn om persoonsgegevens in stukken op te nemen die bestemd zijn voor het college, dan wordt vooraf een afweging 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, kunnen de persoonsgegevens ook worden opgenomen in een geheime bijlage of kan zelfs het hele document geheim worden gehouden. Het is goed om te realiseren dat persoonsgegevens niet alleen hoeven te slaan op de inwoners van de gemeente, maar ook op medewerkers. Ook hun gegevens moet zoveel mogelijk buiten verdere openbaring blijven.

Bij collegestukken zijn het collegebesluit en het voorblad openbaar (tabblad 'registreren' in het Zaaksysteem). 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 Lopik is erop gericht om geen persoonsgegevens in openbare stukken op te nemen, tenzij het een bewuste keuze is dat wel te doen.

3.2 Privacy op ambtelijk niveau

De feitelijke verwerking van persoonsgegevens vindt plaats binnen de ambtelijke organisatie op teamniveau. 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 zoals gebleken is uit hoofdstuk 2. Het is niet meer dan logisch dat een deel van de bevoegdheden en verantwoordelijkheden op het gebied van de privacy dat ligt bij het college, wordt gemandateerd naar de ambtelijke organisatie, specifiek de directie. Deze kan de teamleiders aansturen, zodat zij op effectieve wijze privacy in hun dagelijkse processen kunnen inlijven.

Op die manier worden teamleiders primair verantwoordelijk om passende technische en organisatorische maatregelen te treffen om de rechten van betrokkenen te waarborgen en de verwerking in overeenstemming te brengen met de AVG. De technische maatregelen behelzen voornamelijk het organiseren van de autorisaties. De organisatorische maatregelen hebben betrekking op het bewust omgaan met persoonsgegevens en het treffen van voorzieningen waardoor medewerkers hun taken kunnen blijven uitvoeren.

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

- Inrichten van de werkprocessen in overeenstemming met AVG.
- Bepalen van het doel en middel van de verwerking.
- Toewijzen van middelen in termen van menskracht en geld voor onder andere bewustwordingssessies.
- Bepalen van (mede)verantwoordelijkheid voor de verwerking.
- Inwinnen van advies voorafgaand aan het verstrekken van persoonsgegevens aan een externe partij.
- Voorbereiden van verwerkingsrelaties, protocollen en verwerkingsovereenkomsten opstellen (al dan niet als onderdeel van de samenwerkingsovereenkomst).
- Ondertekenen van protocollen en verwerkingsovereenkomsten.
- Technische infrastructuur voor de verwerkingen.
- Archivering.
- Inzetten Data Protection Impact Assessment (DPIA) of soortgelijke instrumenten om de privacy te toetsen.
- Waarborgen rechten betrokkenen.
- Het tijdig betrekken van de functionaris gegevensbescherming (FG) bij nieuwe of gewijzigde verwerkingen en andere aangelegenheden die verband houden met de bescherming van persoonsgegevens.
- Melden datalekken en andere incidenten.

De teamleiders dragen er ook zorg voor dat medewerkers in het team 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 eedsaflegging. Voor personen die niet in dienst zijn van de gemeente Lopik (bijvoorbeeld Leden van de bezwarencommissie) of medewerkers die tijdelijk worden ingehuurd, geldt dat zij een geheimhoudingsverklaring moeten tekenen. Het template van de geheimhoudingsverklaring is opgenomen in bijlage 3.

Om de portefeuillehouder betrokken te houden en om, samen met het college, de rol van verwerkingsverantwoordelijke in het kader van de privacy waar te maken, wordt periodiek een activiteitenoverzicht gemaakt. Het is de bedoeling om dit activiteitenoverzicht mee te laten lopen met de bedrijfsvoeringsgesprekken of andere bedrijfsvoeringsactiviteiten.

3.3 Functionaris gegevensbescherming

Op grond van artikel 37 AVG wordt een functionaris gegevensbescherming (FG) aangewezen. De verwerkingsverantwoordelijke draagt hierbij zorg dat de FG wordt aangewezen. Deze wordt benoemd op grond van zijn professionele kwaliteiten, 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 Lopik valt de FG steeds formatief onder de gemeentesecretaris.

De FG heeft een informerende en adviserende rol aan de organisatie over verplichtingen die voortvloeien uit de verordening. Daarnaast ziet de FG toe op de naleving van de verordeningsbepalingen en draagt de functionaris zorg voor de privacy-audits. Tot slot fungeert de FG als eerste aanspreekpunt voor de Autoriteit Persoonsgegevens.

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

3.4 Coördinator rechtsbescherming

In geval van een schending dan wel uitoefening van rechten van betrokkenen (zie paragraaf 6.1) moet een betrokkene, los van andere juridische middelen, zich kunnen wenden tot de gemeente als verwerkingsverantwoordelijke.

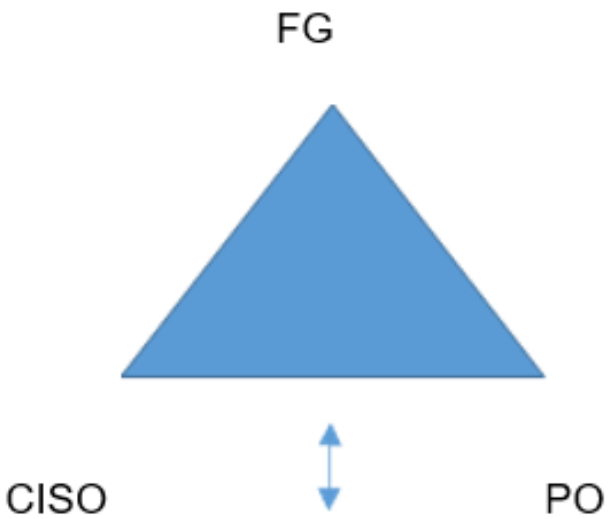
Binnen de gemeente Lopik is steeds een coördinator aangewezen waar verzoeken en bezwaren (ex artikel 21 AVG) kunnen worden ingediend. De coördinator bewaakt de termijn en draagt zorg voor een goede afhandeling van het verzoek of bezwaar. Deze rol wordt vanuit praktisch oogpunt gekoppeld aan die van de privacyofficer.

3.5 Overige functies in kader van privacy

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

Organisatorisch wordt op twee niveaus uitwerking gegeven aan het privacybeleid; directie- en teamniveau.

Op directieniveau vertaalt het zich in een driehoek bestaande uit FG, Chief information and securityofficer (CISO) en een privacy officer (PO). Het doel van de driehoek is om een centrale kennisbank te hebben rond het thema privacy en beveiliging. Alle issues die leven op de werkvloer worden door de driehoek in behandeling genomen en centraal opgeslagen, waarna ze voor iedereen toegankelijk zijn.

Bestuurlijk niveau	Wethouder (portefeuillehouder privacy)
Directieniveau	Directie
	
Teamniveau	Teamleiders

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

Binnen de gemeente Lopik is de PO verantwoordelijk voor het vormgeven en actualiseren van het gemeentelijke privacy-beleid, het doen van organisatorische aanpassingen en draagt er zorg voor dat documenten en andere beslissingen voldoen aan de privacywetgeving. Verder houdt de PO het register van verwerkingen bij. Tot slot fungeert hij als aanspreekpunt voor vragen over toepassing wet- en regelgeving inzake privacy.

Nu teamleiders nadrukkelijk verantwoordelijkheid dragen voor de verwerkingen die in hun team worden verricht, is het zeker in de beginfase wenselijk een persoon binnen het team aan te stellen in de rol van privacy-ambassadeur. De taken die deze medewerker verricht, hangen samen met datgene dat staat opgesomd in paragraaf 3.2. Zo wordt deze medewerker binnen het team als aanspreekpunt belast met de dagelijkse praktijk en schrijft werkinstructies. Uiteraard kan deze medewerker voor ingewikkeldere vraagstukken ondersteuning vragen bij de driehoek.

De functies, rollen en verantwoordelijkheden van CISO, FG en PO zijn vastgelegd in bijlage 1 van het strategisch IBP-beleid.

3.6 Externe relaties/verwerkersovereenkomst
Het verwerken van persoonsgegevens is geen doel op zich, maar staat steeds in het teken van een ander gerechtvaardigd doel dat met die verwerking wordt bereikt (zoals het verlenen van zorg, het houden van toezicht of het uitbetalen van salarissen).

Verwerkersovereenkomst
De gemeente heeft de keuze om de verwerking zelf uit te voeren, dan wel op basis van inkoop, samenwerking, etc. buiten de deur te beleggen. Voor persoonsgegevens waar de gemeente verantwoordelijk voor is, maar die niet door de gemeente worden verwerkt, geldt dat er afspraken moeten worden gemaakt die worden vastgelegd in een verwerkersovereenkomst. Zo wordt met ICT-dienstenleveranciers of zorgverleners een overeenkomst aangegaan en waarbij de gemeente als verantwoordelijke verplichtingen oplegt over passende technische en organisatorische maatregelen. Op grond van het tweede lid van artikel 30 AVG moet een overzicht worden gemaakt van de bestaande verwerkersrelaties.

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 het ook nog denkbaar dat de persoonsgegevens die door de gemeente 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 is geregeld.

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 respectievelijk hun 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. In bijlage 2 bij dit privacybeleid is een voorbeeldprotocol gevoegd.

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 bieden met betrekking tot het toepassen van passende technische en organisatorische maatregelen opdat de verwerking voldoet aan de eisen van de AVG.

De gemeente 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 maakt de gemeente in deze situaties gebruik van verwerkersovereenkomsten. Het gebruik van verwerkingsovereenkomsten is een verplichting die voortvloeit uit de AVG. De verwerkingsovereenkomst is vormvrij en kan dus ook worden geregeld in de bovenliggende overeenkomst tot samenwerking, opdracht, dienstverlening etc. Een template voor de verwerkersovereenkomst is beschikbaar op het intranet.

C. Overdracht van persoonsgegevens aan een andere verwerkingsverantwoordelijke
Daar waar het gaat om een overdracht van de persoonsverwerking (bijvoorbeeld in de vorm van bestanden) aan een andere verwerkingsverantwoordelijke is na overdracht geen gebondenheid meer van de gemeente Lopik. De inspanning van de gemeente Lopik blijft hier beperkt tot het vaststellen of de ontvangende partij daadwerkelijk verwerkingsverantwoordelijke is. Een dergelijk situatie doet zich vaak voor in het Sociaal Domein waar zorginstellingen, SVB, AMHK in de wet als verwerkingsverantwoordelijke zijn aangewezen. Ook in deze situatie is het overdrachtsprotocol als genoemd in bijlage 2 een passende oplossing.

3.7 Samenwerking in de regio
De gemeente Lopik werkt veel samen met andere overheidsinstanties in de regio. Ook deze instanties moeten voldoen aan de vereisten uit de AVG, zoals het aanstellen van een FG en het hebben van een register van verwerkingen. Vaak voeren deze overheidsinstanties een eigen (wettelijke) taak uit en zijn voor de AVG verwerkingsverantwoordelijk (ook al bestaat het bestuur uit wethouders van de deelnemende gemeenten). Samenwerkingsverbanden als hier bedoeld, kunnen ontstaan uit gemeenschappelijke regelingen, maar kunnen ook overheidsbv's zijn.

De AVG legt geen beperkingen op aan het samenwerken en legt bij elke overheidsinstantie zelf de verantwoordelijkheid neer om compliant te zijn voor de AVG. Gelet op het feit dat het, ingeval van samenwerking tussen de gemeente Lopik en de andere instantie, vaak om twee zelfstandig verantwoor-

delijken gaat, hoeft er geen verwerkersovereenkomsten gesloten te worden. Het is wel goed om bij overdracht van persoonsgegevens een overdrachtsmoment af te spreken om de aansprakelijkheid goed te verdelen. Dit kan door middel van het eerdergenoemde protocol uit bijlage E.

4. Werkprocessen

In dit hoofdstuk staat de vraag centraal op welke wijze de gemeente Lopik de verwerking van persoonsgegevens vormgeeft in bedrijfsprocessen en op welke wijze medewerkers gebruik kunnen maken van databases.

In 4.1 wordt het kader geschetst hoe verwerking van persoonsgegevens in de bedrijfsprocessen moet worden ingebed. In 4.2 wordt een bijzondere toepassing van verwerking van persoonsgegevens besproken waar hulpverleners en veiligheidsadviseurs mee te maken hebben in de dagelijkse praktijk. 4.3 gaat dieper in op triages die hoofdzakelijk voorkomen in het sociaal domein.
4.4 bespreekt het gebruik van BSN (een persoonsgegeven o.g.v. Uitvoeringswet AVG). In 4.5 wordt dieper ingegaan op het verwerkingenregister dat door de gemeente Lopik is aangelegd en op basis waarvan de FG zijn toezicht kan effectueren. In de laatste paragraaf wordt besproken hoe met een Data Protection Impact Assessments (DPIA) privacyrisico's van gegevensverwerkingen in beeld gebracht worden en hoe deze vervolgens worden vertaald in het werkproces.

4.1 Inbedding in primaire processen

De AVG eist dat voor de verwerking van persoonsgegevens de beginselen inzake verwerking van persoonsgegevens in acht worden genomen. Deze beginselen vloeien voort uit artikel 5 en 6 AVG (zie voor verdere uitleg Hoofstuk 4 van dit privacybeleid).

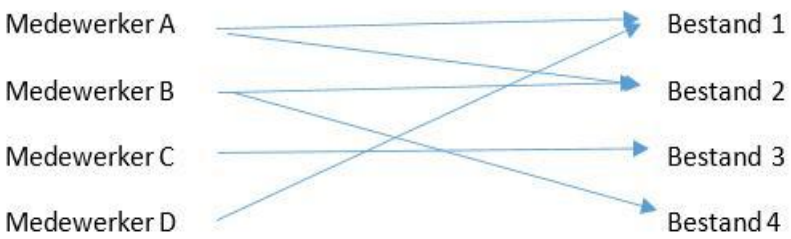
Zo moet de verwerking van persoonsgegevens kunnen steunen op welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Voor werkprocessen binnen de gemeente Lopik betekent dit dat bij verwerkingen een geldige reden moet zijn om de inperking van het grondrecht privacy te rechtvaardigen. Ontbreekt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

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

De organisatiestructuur wordt weerspiegeld in de database met gebruikersaccounts. Deze "Active Directory (AD)" zorgt ervoor dat medewerkers bij documenten, bestanden en applicaties kunnen.

Er wordt aansluiting gezocht bij artikel 6 AVG (zie ook paragraaf 4.4). Voor de gemeente Lopik betekent dat, dat veel verwerkingen als grondslag de goede vervulling van een publieke taak kennen (art. 6.1(e) AVG). In bijzondere gevallen moet een beroep op een van de andere grondslagen, ten finale mogelijkheid toestemming, worden gedaan. Een voorbeeld van toestemming als grondslag is bij het plaatsen van informatie en/of foto's in het smoelenboek op intranet.

Schematische weergave van verdeling takenpakket en toegang tot gegevensbestanden:



Uitgangspunt zijn de taken die door de medewerkers worden uitgevoerd. Deze taken vloeien voort uit functieomschrijvingen. Om in bestanden verwerkingen uit te kunnen voeren, moet men toegang tot die bestanden hebben door middel van autorisatie (waar het om digitale bestanden gaat). Vanaf het moment dat er wordt overgestapt op Office 365 krijgt iedere bestandsmap een eigenaar. Deze eigenaar heeft vervolgens de mogelijkheid om personen te autoriseren om in die map te kunnen. Het is niet aannemelijk dat de teamleider per definitie toegang moet hebben, dit is ook weer afhankelijk van zijn takenpakket.

4.2 Samenwerken met collega's
Binnen de gemeentelijke organisatie hebben medewerkers een takenpakket dat bepalend is voor de toegang tot bestanden. Binnen takenpakketten kan er wel een onderscheid zijn in de diepte waarmee men toegang moet hebben tot de bestanden. Met name in het Sociaal Domein (mogelijk ook elders) kan het wenselijk zijn dat veel medewerkers een kleine hoeveelheid persoonsgegevens kunnen inzien en dat vervolgens een paar medewerkers de totale omvang van de persoonsgegevens (vastgelegd in bijvoorbeeld een dossier) mogen inzien. Ter verduidelijking. De KCC-medewerker moet de NAW-gegevens hebben om door te kunnen verwijzen naar de juiste medewerker, de Wmo-consulent moet naast NAW-gegevens ook de dossierinformatie kunnen inzien om optimale hulp te kunnen verlenen.

Het verdelen van de diepte van de toegang wordt waar mogelijk langs de lijn 'dat-wat' gelegd. Medewerkers (zoals voornoemde KCC-medewerker) kunnen worden geautoriseerd voor de dat-informatie (men weet dat er wat speelt om vervolgens door te kunnen verwijzen) en medewerkers (zoals voornoemde WMO-consulent) die geautoriseerd worden voor de dat-wat-informatie. Zij kunnen het gehele dossier inzien.

Autorisatieschema:

Algemene persoonsgegevens 'dat-informatie'		
Wmo-dossiers 'wat-informatie'	Schuldhulpdossiers 'wat-informatie'	Jeugddossiers 'wat-informatie'

4.3 Triage
Aparte aandacht verdient het proces rond de triage. Uitgangspunt in hulpverlening is om zoveel mogelijk te handelen vanuit 1Gezin,1Plan,1Regisseur (1G1P1R). Triage speelt op casusniveau en vraagt van de medewerker om een professionele inschatting te maken wat de ernst is van de problematiek en welke verwerking van persoonsgegevens daarbij wenselijk is. Met name bij een multi-probleemsituatie 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. Triage doorsnijdt aldus de 1G1P1R-gedachte.

Medewerkers bepalen per casus het doel waarvoor de gegevensverwerking noodzakelijk is voor optimale hulp. 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. Triagemomenten worden benoemd in het werkproces. Gaandeweg het proces waarin hulpverlening wordt geboden aan het gezin waarbij meerdere hulpverleners betrokken zijn, worden vanuit deze triage overlegmomenten georganiseerd waarin persoonsgegevens worden uitgewisseld. Deze overlegmomenten worden gedocumenteerd, zodat het voor de FG duidelijk is welke uitwisseling van persoonsgegevens heeft plaatsgevonden.

De grondslag voor triage is voor de gemeente Lopik het uitvoeren van een publiekrechtelijke taak. 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 het uitvoeren van een dergelijke taak. Medewerkers van de gemeente Lopik moeten er rekening mee houden dat het delen van persoonsgegevens met professionele hulpverleners samenhangt met diens geheimhoudingsplichten (en dus niet alles gedeeld mag worden).

4.4 Gebruik Burgerservicenummers (BSN)
Er is nog veel onduidelijkheid over het gebruik van het BSN in werkprocessen. De regel is dat overheidsorganisaties het BSN mogen gebruiken om hun taak uit te voeren, mits het BSN hierbij noodzakelijk is. Organisaties buiten de overheid mogen het BSN alléén gebruiken als dit in de wet staat en dan alleen voor de doelen die in de wet staan. Zo liet een kinderdagverblijf ouders inloggen op een online ouderportaal met hun BSN. Dat mag niet. Kinderdagverblijven mogen weliswaar naar het BSN van ouders vragen, maar zij mogen dit vervolgens alleen gebruiken voor de kinderopvangtoeslag.

Het voorbeeld van het kinderdagverblijf komt ook regelmatig terug in gemeentelijke processen. Zo mag de gemeente een BSN niet gebruiken als briefkenmerk of dossiernummer. De gemeente mag ook niet standaard om een BSN vragen of een BSN laten vermelden in brieven die men naar de gemeente stuurt.

Het is vaak niet nodig dat de gemeente een BSN opneemt in aan burgers gerichte brieven. In dat geval mag het dan ook niet. Wel kan de gemeente vragen om een BSN te vermelden bij bepaalde verzoeken of vragen.
Dat mag alleen als zo'n verzoek of vraag gaat over een persoonlijke situatie waarbij de medewerker duidelijk wil vaststellen om wie het gaat. Als men een algemene vraag heeft aan de gemeente, bijvoorbeeld over afval, dan hoeft er geen BSN vermeld te worden.

Om BSN in goede banen te leiden wordt apart onderzoek gedaan naar het verwerken van persoonsgegevens met BSN of aan de hand van BSN. De insteek is om vanuit het register van verwerkingen die bestanden te selecteren waarbij BSN in het spel is en hiervoor separaat een DPIA op uit te voeren.

4.5 Verwerkingsregister
Zoals in paragraaf 3.2 is aangegeven ligt de ambtelijke verantwoordelijkheid voor het verwerken van persoonsgegevens bij de teamleiders voor dat deel wat onder hun team valt. Zij brengen in beeld en bewaken het overzicht van de gegevensverwerkingen die in het team plaatsvinden.

Het kader van het overzicht wordt gevormd door artikel 30 van de AVG. Zo moet onder andere vastgesteld zijn dat de verwerking een gerechtvaardigd doel kent en gebaseerd is op een rechtmatige grondslag. De verwerkingen worden bijgehouden in een register. Zie als voorbeeld hieronder de spreadsheet met enkele belangrijke kolommen:

	A	B	C	D	E	F	G	H	I	J	K	L
1	Naam van de verwerking	Contact-gegevens	Categorieën betrokkenen	Categorieën persoons-gegevens	Doelen	Grondslag	Ontvangers intern	Ontvangers extern	Doorgifte landen buiten de EU/EER met waarborgen	Beveiligings-maatregelen	Bewaartermijn	Overig
2	Bijv.: naam van een concrete administratie	Gegevens verwerkings-verantwoor-delijke(n).	Groepen personen waarvan je gegevens verwerkt	Soort gegegevens (naw, contact, financieel etc.)	Per categorie: waarom verwerk je deze specifieke gegevens.	Zie AVG/art. 6: wettelijke grondslag zoals toestemming betrokkene of uitvoering overeenkomst.	Wie binnen de organisatie heeft toegang en mag toegang hebben tot de gegevens.	Welke derden hebben toegang en mogen toegang hebben tot de gegevens.	Zie AVG/art.45-49 indien relevant: denk aan doorgifte gegevens naar moederbedrijf buiten de EU of cloudopslag.	Maatregelen die specifiek zijn voor deze verwerking. Of verwijs naar organisatie-breed beveili-gingsbeleid.	Welke interne criteria gelden voor het wissen van persoons-gegevens.	Bijvoorbeeld gemaakte afspraken met derden en hoe je betrokkenen informeert.
3												
4												
5												
6												

Het overzicht van gegevensverwerkingen wordt geleverd aan de PO die een register bijhoudt van alle verwerkingen van persoonsgegevens binnen de gemeente Lopik. Aan de hand van het register van verwerkingen houdt de FG toezicht op het totaal aantal verwerkingen binnen de gemeente.

4.6 Data Protection Impact Assessment
Wanneer een organisatie persoonsgegevens wil verwerken en dit waarschijnlijk een hoog privacyrisico oplevert, is de organisatie verplicht om een risicoanalyse uit te voeren: een "Data Protection Impact Assessment (DPIA)".

Een DPIA is niet altijd nodig. Naast een lijst van verwerkingen waarvoor de DPIA verplicht is, is er ook een lijst met 9 criteria waarmee het al dan niet uitvoeren van een DPIA kan worden onderbouwd. Deze beoordeling wordt vaak aangeduid als de "Pre-DPIA".

De DPIA's worden uitgevoerd onder leiding van de PO / FG. De proceseigenaren zijn eindverantwoordelijk voor het uitvoeren van DPIA's. Zij maken de keuzes in het bepalen van de restrisico's en welke mitigerende maatregelen genomen worden.

4.7 Bewustwording
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 moet worden omgegaan met de belangen van personen die persoonsgegevens aan de gemeente Lopik 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 Lopik wordt veel aandacht gegeven aan het bewustwordingsproces.

Momenteel is binnen de gemeente Lopik volop aandacht voor het thema privacy. Samen met de CISO en de PO werkt de FG aan het compliant maken van de organisatie voor de AVG. In dat licht worden er ook bewustwordingsacties ontwikkeld. De bewustwordingsacties volgen de voortgang van het beleidsproces.

Voor een aantal verwerkingen van persoonsgegevens worden de komende tijd DPIA's uitgevoerd. De DPIA wordt begeleid door de PO / FG en ingevuld tezamen met medewerkers van de teams. Het doel om met medewerkers DPIA's uit te voeren is tweeledig; betrokkenheid vergroten en het verzorgen van een leereffect, zodat sommige medewerkers later zelf een DPIA kunnen uitvoeren.

Dit privacybeleid vormt ook een bron voor communicatie naar de teams. Na vaststelling van het tactisch privacybeleid wordt het met de teams besproken. Met de teamleiders wordt vervolgens een lijn uitgedacht om jaarlijks activiteiten rond het thema 'privacy en informatieveiligheid' te bedenken met daarin aandacht voor bewustwording en gegevensbeveiliging.

Het uitgangspunt van het jaarlijkse activiteitenplan is om het bewustwordingsproces zo dicht mogelijk bij de medewerkers te organiseren. Welke communicatiemiddelen en trainingen worden ingezet, ligt bij de teamleiders.

4.8 Beheer en opslag van persoonsgegevens

4.8.1 Opslag van persoonsgegevens

Persoonsgegevens worden binnen de gemeente Lopik (vrijwel) altijd digitaal opgeslagen. Voor opslag van gegevens beschikt de gemeente Lopik over een eigen, afgeschermd netwerk. De manier waarop gemeente Lopik haar netwerk en gegevens beveiligd is in overeenstemming met de gemeentelijke beveiligingsnormen (BIO, zie ook 2.2.6)
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 in de gemeente Lopik opgenomen in centrale databases.
- Binnen decentrale databases en spreadsheets die door algemene kantoorautomatiseringssoftware te benaderen zijn. Dit betreft kleinschalige registraties met een zeer specifiek doel.
- Op ongestructureerde basis: in documenten, afbeeldingen 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 geschiedt op goed beveiligde netwerken waarover de gemeente Lopik dient te beschikken.
- Aan medewerkers die geregeld met persoonsgegevens op pad gaan wordt een beveiligde voorziening aangeboden (smartphone, notebooks).
- Lokale opslag zoals smartphones en laptops worden afdoende versleuteld.

De gemeente Lopik 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-upt. Ook deze maatregelen zijn in lijn met de gemeentelijke beveiligingsnormen.

4.8.2 Toegang tot en beheer van persoonsgegevens

Alleen geautoriseerde personen hebben toegang tot het netwerk van gemeente Lopik 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 persoonsgegevens is vastgelegd in hoeverre deze vanuit de rol ingezien en mogen worden veranderd. De toewijzing van rollen aan medewerkers wordt vastgelegd in autorisatiematrices en periodiek gecontroleerd.

De benodigde toegangsrechten worden vastgesteld door de teamleiders. Zij zijn verantwoordelijk voor de verwerking van persoonsgegevens (zie ook paragraaf 3.2) 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 hiervoor een formele procedure. Toegang tot persoonsgegevens wordt op gegevens- en medewerkersniveau geregistreerd (gelogd). Op deze manier is te achterhalen wie op welk tijdstip welke gegevens heeft geraadpleegd. De gemeente Lopik kent procedures om deze login te gebruiken bij privacyincidenten.

GEMEENTE LOPIK

5. Vaststelling

Vastgesteld in de vergadering van 19 december 2023

de gemeentesecretaris,
drs. F. Jonker

de burgemeester,
dr. L.J. de Graaf