GEMEENTE LOPIK

# GEMEENTEBLAD

Officiële uitgave van de gemeente Lopik

Nr. 45788

26 februari 2019

## Besluit van het college van burgemeester en wethouders van de gemeente Lopik houdende regels omtrent veilig omgaan met persoonsgegevens in de gemeente Lopik

Het college van burgemeester en wethouders van de gemeente Lopik,

gezien het advies van de afdeling Bedrijfsvoering van 7 januari;

overwegende dat het College waarde hecht aan het voldoen aan de eisen die de op 25 mei 2018 inwerking getreden Algemene Verordening Gegevensbescherming aan de gemeente Lopik oplegt en het Beleidsplan Privacy hiertoe zowel een strategisch kader, alsook een concreet actieplan biedt;

**besluit:**

1. ‘Beleidsplan veilig omgaan met persoonsgegevens in de gemeente Lopik’ vast te stellen en daarmee in te stemmen met de acties zoals vermeld in bijlage 4 van het beleidsplan (onder voorbehoud dat ook de OR hiermee instemt over het gedeelte dat gaat over de verwerking van persoonsgegevens van personeelsleden);
2. het Beleidsplan Privacy ter kennisname naar de Raad te sturen.

### 1. Inleiding

In de afgelopen decennia hebben technische ontwikkelingen een hoge vlucht genomen. Het is steeds eenvoudiger geworden om informatie, waaronder informatie over personen, via ICT-middelen te delen met anderen, op te slaan in bestanden of te combineren met andere informatie die (vanuit openbare bronnen) beschikbaar is.

In de Wet Bescherming Persoonsgegevens van 6 juli 2000 (afgeleid van de Europese databeschermingsrichtlijn uit 1995) is een eerste poging gedaan om op nationaal niveau grip te krijgen op het verwerken van persoonsgegevens. Deze wet stamt uit een tijd dat ICT-middelen nog een beperkte invloed hadden op de maatschappij en men zich onvoldoende realiseerde dat informatie, waaronder informatie over personen, zich eenvoudig tot buiten de landsgrenzen kon verspreiden. Zeker met de cloudtoepassingen die we nu kennen, is het onmogelijk geworden om te traceren waar informatie over personen zich daadwerkelijk bevindt.

Op 21 oktober 2013 is de Algemene Verordening Gegevensbescherming (AVG) aangeboden aan het Europese Parlement. Nadat deze op 25 mei 2016 in werking is getreden, hebben nationale overheden bedrijven en overheidsinstanties 2 jaar de tijd gegeven om aan de bepalingen van de AVG te voldoen.

Het belang van het hebben van goede bepalingen over het beschermen van persoonsgegevens is terug te voeren op andere verdragsrechtelijke en grondwettelijke bepalingen die bescherming bieden aan de persoonlijke levenssfeer, waaronder het beschermen van persoonsgegevens. Zo luidt artikel 8 van het Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden:

*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, en luidt artikel 10 van de Grondwet:

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 AVG 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 wetswijzigingen 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 AVG in werking getreden en moeten verwerkingsverantwoordelijken (waaronder gemeenten) sinds 25 mei 2018 aan de Verordening voldoen. De Wet Bescherming Persoonsgegevens wordt voor een deel overgeheveld naar de Uitvoeringswet Algemene Verordening Gegevensbescherming en voor het overige 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.

Het plan geeft invulling aan de wens van de Lekstroomgemeenten om op het terrein van privacy gezamenlijk op te trekken. Dit beleidsplan is voor de gemeenten Houten, Nieuwegein, IJsselstein, Montfoort en Lopik in grote lijnen gelijkluidend, maar kennen elk een eigen lokale kleur. Het grote voordeel van het hebben van een gezamenlijk uitgangspunt is dat het de communicatie over privacy tussen de gemeenten vereenvoudigd heeft.

Dit plan is met een zekere abstractie geschreven en biedt vooral een denkrichting aan. Bij de feitelijke invulling van het plan door de afzonderlijke gemeenten is meer ruimte voor een eigen inbreng en zullen de teams nadrukkelijk betrokken worden bij de verdere inrichting van de werkprocessen, het beheer en de opslag van de gegevens en zal er voldoende aan bewustwording worden gedaan.

Voldoen aan de AVG betekent dat op verschillende terreinen binnen de gemeentelijke organisatie aandacht moet zijn voor privacy. Het toverwoord in de AVG is compliance. Bedrijven en overheidsinstanties moeten aantonen dat zij inspanningen hebben gedaan om aan de wet- en regelgeving te voldoen. Om die reden worden governance, beleid, werkprocessen en triages, bewustwording en het beheer en opslag van gegevens onder de loep genomen die mogelijk leiden tot aanpassing van processen of werkafspraken. In dit beleidsplan zijn ook de aanbevelingen uit het rekenkameronderzoek meegenomen.


Daarnaast worden allereerst een aantal begrippen en het algemene kader voor gegevensverwerking besproken. Vervolgens wordt 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 dieper ingegaan op beheer en opslag van persoonsgegevens.

Voorafgaand aan dit beleidsplan is door onderzoeksbureau A3PConsultancy onderzoek gedaan naar de stand van zaken van het privacykader. Hoewel er accenten zijn aan te geven tussen de onderzoeksrapporten van de Lekstroomgemeenten is er wel een gemeenschappelijke lijn te ontdekken. De aanbevelingen die uit de verschillende rapportages zijn gekomen, zijn meegenomen in dit beleidsplan en worden ter uitwerking van dit plan in werkinstructies opgenomen. Zie bijlage 4 voor het overzicht van de activiteiten die moeten worden uitgevoerd na vaststelling van het beleidsplan.

GEMEENTE LOPIK

## 2. College samenvatting

Volgens de AVG is het college van burgemeester en wethouders (soms de raad of burgemeester alleen) verwerkingsverantwoordelijk en zijn zij gehouden aan de verordening te voldoen. Deze bestuurlijke verantwoordelijkheid wordt voor de dagelijkse sturing belegd bij de portefeuillehouder informatiebeleid, waar ook privacy onder valt.

Waar het gaat om het beschermen van persoonsgegevens geeft de AVG duidelijk richting aan. Persoonsgegevens mogen slechts worden verwerkt als er een doel mee gediend is en er een rechtsgeldige grondslag geldt. De wetgever heeft het vervolgens aan de verantwoordelijkheid van de verwerker overgelaten hoe zij tot doelbepaling en vaststelling van grondslagen komen. Gelet op het uiteenlopende takenpakket van gemeenten en de grote aantallen gegevensbestanden dat in dat licht wordt verwerkt , zijn er veel doelen aan te wijzen waarvoor gemeenten persoonsgegevens verwerkt. Randvoorwaarde hierbij is wel dat bij de bepaling van het doel moet worden nagedacht over bijvoorbeeld toereikendheid, rechtmatigheid en dataminimalisatie.

In de praktijk is privacy een issue 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 de afdelingshoofden. Op bedrijfsniveau bieden de functionaris gegevensbescherming, de coördinator informatieveiligheid en de juridisch privacy-adviseur ondersteuning bij het inrichten van de kaders, zij zijn adviseurs voor technische en organisatorische kwesties en hebben een coördinerende rol in de bedrijfsvoeringscyclus en het verwerken van datalekken. De invulling van het thema privacy op de werkvloer wordt gedaan met de bestaande formatie; er bestaat op dit moment geen behoefte aan uitbreiding.

De ruimte voor zelfstandig beleid is beperkt. Belangrijke beleidsthema's die spelen zijn in hoofdstuk 6 van dit beleidsplan verder uitgewerkt. De gekozen beleidsoplossingen vloeien voort uit de AVG, afzonderlijke materiewetten of jurisprudentie.

Waar het gaat om bedrijfsprocessen, genoemd in hoofdstuk 7, wordt aansluiting gezocht bij een belangrijk uitgangspunt van de AVG op dit punt. Alleen voor het uitvoeren van specifieke taken hebben medewerkers toegang tot bepaalde bestanden. Om dit mogelijk te maken wordt een autorisatieschema opgesteld voor die toegang en wordt nagedacht over het op tijd toelaten en afsluiten van medewerkers tot die bestanden.

Bewust omgaan met persoonsgegevens wordt binnen de organisatie een vast thema. Aan de hand van verschillende leer- en communicatiemiddelen worden medewerkers meegenomen om bewuster met de privacy van betrokkenen om te gaan. De communicatie over bescherming persoonsgegevens gecombineerd wordt informatieveiligheid binnen de gemeente Lopik.

Bij de opslag en beheer van persoonsgegevens is met name gekeken hoe deze het beste beveiligd kunnen worden, gebruikmakend van de bestaande ICT-infrastructuur aangevuld met beveiligde devices voor gebruik buitenshuis.

In dit beleidsplan worden onder meer de aanbevelingen uit het onderzoek van A3PConsultancy meegenomen zodat nu, samen met een groot aantal andere aspecten, een integraal beleidsplan privacy wordt gepresenteerd.

## 3. Begrippen

In dit beleidskader worden verschillende begrippen geïntroduceerd met een zekere lading 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;
- T oestemming 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 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 afdeling 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 afdeling 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 t. Deze verwerkingen moeten om die reden worden beëindigd.


### 4.2. 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 afdelingsniveau moet per verwerking worden vastgesteld welke persoonsgegevens ten minste noodzakelijk zijn om het doel te kunnen bereiken.

### 4.3. 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 verwerkelijkt (bijvoorbeeld het verkrijgen van de informatie uit open data).

Ook hier moet per afdeling 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.

### 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:
- 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.

### 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 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 door de verwerkingsverantwoordelijke bepaald. 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 beleidsplan 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.

### 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 Lopik wordt aan deze eis van passende maatregelen invulling gegeven door het invoeren van de maatregelenset van de Baseline Informatiebeveiliging Gemeenten (BIG). Deze baseline is ontwikkeld door VNG/KING. 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 bovenop 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 BIG wordt in verschillende varianten binnen de overheid gebruikt en zijn gebaseerd op de internationale beveiligingsstandaarden ISO 270001 en ISO 270002.

## 5. Governance

Om te voldoen aan de AVG zijn op bestuurlijk en ambtelijk niveau binnen de gemeente Lopik een aantal organisatorische maatregelen noodzakelijk. 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 Lopik.

### 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 door de gemeente Lopik belegd bij een van de portefeuillehouders die als vast aanspreekpunt fungeert voor privacy-issues.
Bij de gemeente Lopik is dat wethouder Spelt. Op bestuurlijk niveau blijft dan allen 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 afdelingsniveau 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 er op gericht om geen persoonsgegevens in openbare stukken op te nemen, tenzij het een bewuste keuze is dat 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 zoals gebleken is uit hoofdstuk 4. 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. Het afdelingshoofd bedrijfsvoering is de meest aangewezen persoon om te belasten met privacy-issues. Vanuit de rol van ambtelijk opdrachtgever kan deze persoon afdelingsmanagers aansturen, zodat zij op effectieve wijze privacy in hun dagelijkse processen kunnen inlijven.

Op die manier worden afdelingsmanagers 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 afdelingsmanagers 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;
- 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 privacy impact assessment (PIA) of soortgelijke instrumenten om de privacy te toetsen,
- waarborgen rechten betrokkenen;
- melden van verwerkingen bij de functionaris gegevensbescherming (FG); - melden datalekken en andere incidenten.

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 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.

### 5.3. 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.

### 5.4. 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.

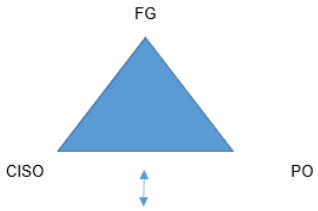
### 5.5. Overige functies in kader van privacy
Buiten de in de AVG met naam genoemde functie van FG houden binnen de gemeente Lopik ook anderen zich nadrukkelijk bezig met de dagelijkse praktijk rond privacy.

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

Op bedrijfsvoeringsniveau vertaalt het zich in een driehoek bestaande uit FG, Chief information and securityofficer (CISO) en een privacyofficer (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)

Bedrijfsvoeringsniveau Manager bedrijfsvoering




Afdelingsniveau Afdelingsmanagers

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 er voor 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 en het register van verwerkers bij. Tot slot fungeert hij als aanspreekpunt voor vragen over toepassing wet- en regelgeving inzake privacy.

Nu afdelingsmanagers nadrukkelijk verantwoordelijkheid dragen voor de verwerkingen die op hun afdeling worden verricht, is het zeker in de beginfase wenselijk een persoon vrij te maken voor het thema privacy binnen dat team. De taken die deze medewerker verricht, hangen samen met datgene dat staat opgesomd in paragraaf 5.2. Zo wordt deze medewerker binnen de afdeling als aanspreekpunt belast met de dagelijkse praktijk en schrijft werkinstructies. Uiteraard kan deze medewerker voor ingewikkeldere vraagstukken ondersteuning vragen bij de driehoek.

### 5.6. 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 ICTdienstenleveranciers 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 beleidsplan 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. Om een beeld te hebben van de wijze waarop de relatie tussen verwerkingsverantwoordelijke en verwerker moet worden vormgegeven is een template verwerkersovereenkomst als bijlage 1 bij dit beleidsplan opgenomen.

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.

### 5.7. 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; het aanstellen van een FG, het hebben van een register van verwerkingen, etc.. Vaak voeren deze overheidsinstanties een eigen (wettelijke) taak uit en zijn voor de AVG verwerkingsverantwoordelijke (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 verantwoordelijken 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 eerder genoemde protocol uit bijlage E.

## 6. Privacybeleid

In de AVG wordt 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 Lopik hecht er waarde aan dat de persoonsgegevens die aan haar zijn toevertrouwd alleen worden gebruikt 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 worden genomen, moeten duidelijk worden gemotiveerd.

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

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

### 6.1. 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;
   - het recht op rectificatie en gegevenswissing;
   - het recht om een klacht in te dienen bij de toezichthoudende autoriteit;
   - (indien gegevens niet bij betrokkene worden verzameld) informatie over de bron van de gegevens; - 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 5.4) begeleid.

### 6.2. 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. Dit kan geschieden door zijn naam te vermelden op een inlegvel die is toegevoegd aan de agenda. Na afloop van de collegevergadering wordt het inlegvel 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 Wob-verzoeken kunnen de namen van medewerkers achterwege blijven. Uit artikel 10, eerste lid onder de Wob vloeit dit al voort. In het kader van dit beleidsplan 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 Wob-verzoeken afhandelt, betekent dit een extra alertheid.

### 6.3. 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 Privacy Impact Assessment (PIA) 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.

### 6.4. 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.

Beveiligingsincidenten worden nu al gemeld door medewerkers of verwerkers bij de CISO van de gemeente. De CISO maakt een analyse of het beveiligingslek mogelijk ook een datalek is. Bij een vermoeden van een datalek wordt de FG gewaarschuwd. Gelet op het feit dat het al sinds 1 januari 2016 verplicht is om datalekken te melden bij de Autoriteit Persoonsgegevens, heeft de gemeente Lopik inmiddels een ‘werkinstructie meldplicht datalekken’ en wordt dit beleidsthema hier verder onbesproken.

### 6.5. 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.

## 7. 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 7.1 wordt het kader geschetst hoe verwerking van persoonsgegevens in de bedrijfsprocessen moet worden ingebed. In 7.2 wordt een bijzondere toepassing van verwerking van persoonsgegevens besproken waar hulpverleners en veiligheidsadviseurs mee te maken hebben in de dagelijkse praktijk. 7.3 gaat dieper in op triages die hoofdzakelijk voorkomen in het sociaal domein.
7.4 bespreekt het gebruik van BSN (een persoonsgegeven o.g.v. Uitvoeringswet AVG). In 7.5 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 Privacy Impact Assessments (PIA's) privacyrisico's van gegevensverwerkingen in beeld gebracht worden en hoe deze vervolgens worden vertaald in het werkproces.

### 7.1. 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 beleidsplan).

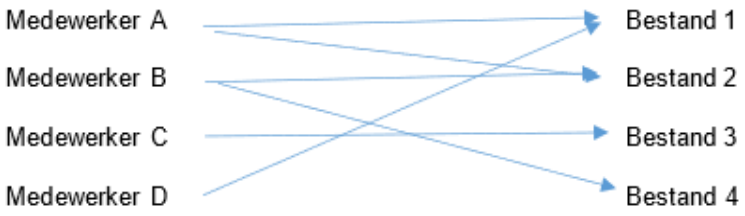
Zo moet de verwerking van persoonsgegevens kunnen steunen op welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Voor werkprocessen binnen de gemeente Lopik betekent dit dat bij verwerkingen een geldige reden moet zijn om de inperking van het grondrecht privacy te rechtvaardigen. Ontbreekt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

Voor een belangrijk deel worden deze uitgangspunten momenteel verwerkt en ingepast in de bestaande organisatie. De huidige stand van zaken is dat eerder dit jaar een organisatiewijziging is doorgevoerd waarbij ook de structuur (inrichting) ten aanzien van rechten en rollen van het computersysteem is aangepast. Deze structuur, de Active Directory (AD), zorgt ervoor dat medewerkers bij documenten, bestanden en applicaties kunnen. Deze structuur werkt op de 'achtergrond'.

In 2019 worden de autorisaties op basis waarvan toegang van medewerkers tot de werkprocessen verder wordt ingevuld, meegenomen in de nieuwe releases van 'Key2Zaken' van Centric.

De volgende stap is dat aansluiting wordt gevonden bij een van de grondslagen uit 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 afdelingsmanager per definitie toegang moet hebben, dit is ook weer afhankelijk van zijn takenpakket.

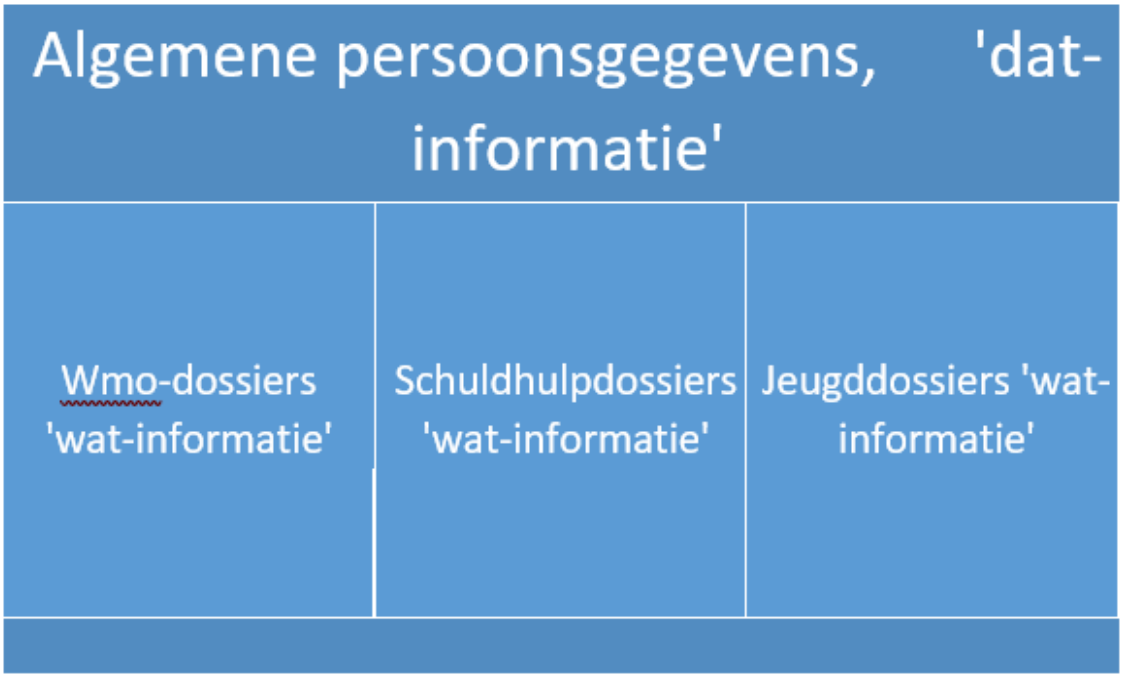
### 7.2. Samenwerken met collega's

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 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:




### 7.3. 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).

### 7.4. Gebruik Burgerservicenummers

Er is nog veel onduidelijkheid over het gebruik van het BSN nummer 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 PIA op uit te voeren.

### 7.5. Verwerkingenregister

Zoals in het hoofdstuk Governance is aangegeven ligt de ambtelijke verantwoordelijkheid voor het verwerken van persoonsgegevens bij de afdelingsmanagers. Zij brengen in beeld en bewaken het overzicht van de gegevensverwerkingen die op de afdeling 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. Uiteindelijke levert dit het volgende plaatje op:

| **Verwerkingsregister** | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | |
| **Taak-verant-woordelijke** | **Naam verwerking/ proces** | **Doel ver-werking** | **Betrok-kenen** | **Persoons-gegevens** | **Bijzondere persoons-gegevens** | **Ont-vangers** | **Grond-slag** | **Bewaar-termijnen** | **Beschrijving beveiligings-maatregelen** |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |

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.

### 7.6. Privacy Impact Assessment

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

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

Het is niet noodzakelijk om voor alle processen waarbij persoonsgegevens worden verwerkt een PIA uit te voeren. Om die reden is er een onderscheid aangebracht en worden in 2019 alleen PIA's uitgevoerd in geval van nieuwe verwerkingen van persoonsgegevens en verwerkingen waarbij sprake is van een

grote verzameling van persoonsgegevens of een verzameling met bijzondere categorieën van persoonsgegevens. Een selectie van verwerkingen waarvoor een PIA wordt georganiseerd vloeit voort uit het verwerkingenregister als genoemd in paragraaf 7.3.

In eerste aanleg worden de PIA's uitgevoerd onder leiding van de kwartiermaker FG en later door de FG.

## 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 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.

### 8.2. Bewustwording

Momenteel is binnen de gemeente Lopik volop aandacht voor het thema privacy. Samen met de CISO en de PO werkt de kwartiermaker 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 PIA's uitgevoerd. De PIA wordt de eerste periode begeleid vanuit de kwartiermaker FG en worden met medewerkers van de teams ingevuld. Het doel om met medewerkers PIA's uit te voeren is tweeledig; betrokkenheid vergroten en het verzorgen van een leereffect, zodat sommige medewerkers later zelf een PIA kunnen uitvoeren.

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

### 8.3. Bewustwording door afdelingsactiviteiten

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 het afdelingsmanagement.

## 9. Beheer en opslag van persoonsgegevens

### 9.1. 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 beveiligt is in overeenstemming met de gemeentelijke beveiligingsnormen (BIG, 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 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.

### 9.2. 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 het afdelingsmanagement. Zij zijn verantwoordelijk voor de verwerking van persoonsgegevens (zie ook paragraaf 5.3) 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.

*Vastgesteld in de vergadering van 15 januari.*

*de gemeentesecretaris,*
*mw. mr. E.T. Halman-van der Linden*

*de burgemeester,*
*dr. L.J. de Graaf*

GEMEENTE LOPIK

## Bijlage 1 Overeenkomst verwerker/ gemeente Lopik ex artikel 28 lid 3 AVG en/of artikel 7 Besluit basisregistratie personen

**Verwerkersovereenkomst**

Het College van Burgemeester en Wethouders van de gemeente Lopik, verder te noemen de verwerkingsverantwoordelijke, ten deze rechtsgeldig vertegenwoordigd door de mevrouw mr. M.J.L. Dukers, hoofd van de afdeling Bedrijfsvoering

en

<Bedrijf, afdeling>, gevestigd te <plaatsnaam>, verder te noemen de verwerker, ten deze rechtsgeldig vertegenwoordigd door de <de heer of mevrouw>, <persoonsnaam> , <functie>,

verklaren te zijn overeengekomen een verwerkersovereenkomst als bedoeld in artikel 14 tweede lid van de Wet Bescherming persoonsgegevens en, vanaf 25 mei 2018, als bedoeld in artikel 28, derde lid, van de Algemene Verordening Gegevensbescherming (hierna: AVG), tussen de verwerkingsverantwoordelijke en de verwerker. Waar in deze verwerkersovereenkomst termen worden gebruikt die overeenstemmen met definities uit artikel 4 AVG, wordt aan deze termen de betekenis van de definities uit de AVG toegekend.

**Artikel 1 Definities**

1.1 Bijlagen: aanhangsels bij deze verwerkersovereenkomst, die na door beide partijen te zijn geparafeerd, deel uitmaken van deze verwerkersovereenkomst.

1.2 Normen en standaarden: de door de verwerkingsverantwoordelijke vastgestelde normen en standaarden ter zake van methoden, technieken, procedures, projecten, productiekenmerken en documentatievoorschriften welke bij de uitvoering van de werkzaamheden door de verwerker zullen worden gevolgd als vastgelegd in bijlage A.

1.3 Toezichthouder: de Autoriteit Persoonsgegevens (AP) is het zelfstandig bestuursorgaan dat in Nederland bij wet als toezichthouder is aangesteld voor het toezicht op het verwerken van persoonsgegevens.

1.4 (Verwerkings)verantwoordelijke: 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.

1.5 Verwerker: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt. Degene die ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt, in opdracht van de verwerker, is een sub-verwerker.

**Artikel 2 Ingangsdatum en duur**

2.1 Deze verwerkersovereenkomst gaat in op het moment van ondertekening en duurt voort zolang de verwerker als verwerker van persoonsgegevens optreedt in het kader van de door de verwerkingsverantwoordelijke ter beschikking gestelde persoonsgegevens voor <nader in te vullen omschreven doel>

**Artikel 3 Onderwerp van deze verwerkersovereenkomst**

3.1 De verwerker verwerkt de door of via verwerkingsverantwoordelijke ter beschikking gestelde persoonsgegevens uitsluitend in opdracht van de verwerkingsverantwoordelijke in het kader van de uitvoering van <contract, nummer>; dit is de onderliggende hoofdovereenkomst. De door de verwerker uit te voeren werkzaamheden waar deze verwerkersovereenkomst betrekking op heeft, worden nader omschreven in bijlage B. Verwerker zal de persoonsgegevens niet voor enig ander doel verwerken, behoudens afwijkende wettelijke verplichtingen.

3.2 De verwerker verbindt zich om in het kader van die werkzaamheden de door of via de verwerkingsverantwoordelijke ter beschikking gestelde persoonsgegevens zorgvuldig te verwerken.

**Artikel 4 Verplichtingen verwerker**

4.1 De verwerker verwerkt gegevens ten behoeve van de verwerkingsverantwoordelijke, in overeenstemming met diens schriftelijke instructies.

4.2 De verwerker heeft geen zeggenschap over de ter beschikking gestelde persoonsgegevens. Zo neemt hij geen beslissingen over ontvangst en gebruik van de gegevens, de verstrekking aan derden en de duur van de opslag van gegevens. De zeggenschap over de persoonsgegevens verstrekt onder deze verwerkersovereenkomst komt nimmer bij de verwerker te berusten.

4.3 De verwerker zal bij de verwerking van persoonsgegevens in het kader van de in artikel 3 genoemde werkzaamheden, handelen in overeenstemming met de toepasselijke wet- en regelgeving betreffende de verwerking van persoonsgegevens. De verwerker zal alle redelijke instructies van de contactpersoon, als bedoeld in artikel 12.2, opvolgen, behoudens afwijkende wettelijke verplichtingen. Indien deze afwijkende wettelijke verplichtingen er zijn wordt de verantwoordelijke hiervan, voorafgaand aan de verwerking, schriftelijk op de hoogte gebracht door de verwerker.

4.4 De verwerker zal te allen tijde op eerste verzoek van de contactpersoon, als bedoeld in artikel 12.2, door verwerkingsverantwoordelijke ter beschikking gestelde persoonsgegevens met betrekking tot deze verwerkersovereenkomst ter hand stellen.

4.5 De verwerker stelt de verwerkingsverantwoordelijke te allen tijde in staat om binnen de wettelijke termijnen te voldoen aan de verplichtingen op grond van de AVG, meer in het bijzonder de rechten van betrokkenen, zoals, maar niet beperkt tot een verzoek om inzage, verbetering, aanvulling, verwijdering of afscherming van persoonsgegevens en het uitvoeren van een gehonoreerd aangetekend verzet.

4.6 De verwerker werkt op verzoek van verwerkingsverantwoordelijke te allen tijde mee aan een gegevensbeschermingseffectbeoordeling (PIA).

**Artikel 5 Geheimhoudingsplicht**

5.1 Personen in dienst van, dan wel werkzaam ten behoeve van de verwerker, evenals de verwerker zelf, zijn verplicht tot geheimhouding met betrekking tot de persoonsgegevens waarvan zij kennis kunnen nemen, behoudens voor zover een bij, of krachtens de wet gegeven voorschrift tot verstrekking verplicht. De medewerkers van de verwerker tekenen hiertoe een geheimhoudingsverklaring.

5.2 Indien de verwerker op grond van een wettelijke verplichting gegevens dient te verstrekken, zal de verwerker de grondslag van het verzoek en de identiteit van de verzoeker verifiëren en zal de verwerker de verwerkingsverantwoordelijke onmiddellijk, voorafgaand aan de verstrekking, ter zake informeren. Tenzij wettelijke bepalingen dit verbieden.

**Artikel 6 Meldplicht datalekken en beveiligingsincidenten**

6.1 De verwerker zal de verwerkingsverantwoordelijke zo spoedig mogelijk - doch uiterlijk binnen 24 uur na de eerste ontdekking - informeren over alle (vermoedelijke) inbreuken op de beveiliging alsmede andere incidenten die op grond van wetgeving moeten worden gemeld aan de toezichthouder of betrokkene, onverminderd de verplichting de gevolgen van dergelijke inbreuken en incidenten zo snel mogelijk ongedaan te maken dan wel te beperken, al dan niet onder verbeurte van een boete in geval van niet-nakoming, conform artikel 10.4 van deze verwerkersovereenkomst. Verwerker zal voorts, op het eerste verzoek van de verwerkingsverantwoordelijke, alle inlichtingen verschaffen die de verwerkingsverantwoordelijke noodzakelijk acht om het incident te kunnen beoordelen.
Daarbij verschaft verwerker in ieder geval de informatie aan de verwerkingsverantwoordelijke zoals omschreven in bijlage C.

6.2 De verwerker beschikt over een gedegen plan van aanpak betreffende de omgang met en afhandeling van inbreuken en zal de verwerkingsverantwoordelijke, op diens verzoek, inzage verschaffen in het plan. Verwerker stelt de verwerkingsverantwoordelijke op de hoogte van materiele wijzigingen in het plan van aanpak.

6.3 De verwerker zal het doen van meldingen aan de toezichthouder(s) overlaten aan de verwerkingsverantwoordelijke.

6.4 De verwerker zal alle noodzakelijke medewerking verlenen aan het zo nodig, op de kortst mogelijke termijn, verschaffen van aanvullende informatie aan de toezichthouder(s) en/of betrokkene(n). Daarbij verschaft verwerker in ieder geval de informatie, zoals beschreven in bijlage C, aan de verwerkingsverantwoordelijke.

6.5 De verwerker houdt een gedetailleerd logboek bij van alle (vermoedens van) inbreuken op de beveiliging, evenals de maatregelen die in vervolg op dergelijke inbreuken zijn genomen waarin minimaal de informatie zoals bedoeld in bijlage C is opgenomen, en geeft daar op eerste verzoek van de verwerkingsverantwoordelijke inzage in.

**Artikel 7 Beveiligingsmaatregelen en controle**

7.1 De verwerker neemt alle passende technische en organisatorische maatregelen om de persoonsgegevens welke worden verwerkt ten dienste van de verwerkingsverantwoordelijke te beveiligen en beveiligd te houden tegen verlies of tegen enige vorm van onrechtmatige verwerking. De wijze van beveiliging wordt nader omschreven in bijlage D.

7.2 De verwerkingsverantwoordelijke is te allen tijde gerechtigd de verwerking van persoonsgegevens te (doen) controleren. De verwerker is verplicht de verwerkingsverantwoordelijke, de Autoriteit Persoonsgegevens, of, de onder geheimhouding, controlerende instantie in opdracht van verwerkingsverantwoordelijke toe te laten en verplicht medewerking te verlenen zodat de controle daadwerkelijk uitgevoerd kan worden.

7.3 De verwerkingsverantwoordelijke zal de controle slechts (laten) uitvoeren na een voorafgaande schriftelijke melding aan de verwerker.

7.4 De verwerker verbindt zich om binnen een door de verwerkingsverantwoordelijke te bepalen termijn de verwerkingsverantwoordelijke, of de door de verwerkingsverantwoordelijke ingeschakelde derde, te voorzien van de verlangde informatie. Hierdoor kan de verwerkingsverantwoordelijke, of de door de verwerkingsverantwoordelijke ingeschakelde derde, zich een oordeel vormen over de naleving door de verwerker van deze verwerkersovereenkomst. De verwerkingsverantwoordelijke, of de door de verwerkingsverantwoordelijke ingeschakelde derde, is gehouden alle informatie betreffende deze controles vertrouwelijk te behandelen.

7.5 Verwerker staat er voor in, de door de verwerkingsverantwoordelijke of ingeschakelde derde, aangegeven aanbevelingen ter verbetering binnen de daartoe door de verwerkingsverantwoordelijke te bepalen redelijke termijn uit te voeren.

7.6 De verwerker rapporteert jaarlijks over de opzet en werking van het stelsel van maatregelen en procedures, gericht op naleving van deze verwerkersovereenkomst.

7.7 Naast rapportages door de verwerker en controles door de verwerkingsverantwoordelijke of controlerende instantie in opdracht van de verwerkingsverantwoordelijke, kunnen beide partijen ook overeenkomen gebruik te maken van een Third Party Memorandum (TPM) opgesteld door een onafhankelijke externe deskundige.

7.8 De redelijke kosten van de controle worden gedragen door de partij die de kosten maakt, tenzij uit de controle blijkt dat de verwerker enig punt uit deze verwerkersovereenkomst niet heeft nageleefd. In dat geval worden de kosten van de controle gedragen door de verwerker.

**Artikel 8 Inschakeling derden**

8.1 De verwerker is slechts gerechtigd de uitvoering van de werkzaamheden geheel of ten dele uit te besteden aan derden na voorafgaande, duidelijk gespecificeerde, schriftelijke toestemming van de verwerkingsverantwoordelijke.

8.2 De verwerkingsverantwoordelijke kan aan de schriftelijke toestemming voorwaarden verbinden, op het gebied van geheimhouding en ter naleving van de verplichtingen uit deze verwerkersovereenkomst.

8.3 De verwerker blijft in deze gevallen te allen tijde aanspreekpunt en verantwoordelijk voor de naleving van de bepalingen uit deze verwerkersovereenkomst. De verwerker garandeert dat deze derden schriftelijk minimaal dezelfde plichten op zich nemen als tussen de verwerkingsverantwoordelijke en de verwerker zijn overeengekomen en zal de verwerkingsverantwoordelijke, op diens verzoek, inzage verschaffen in de overeenkomsten met deze derden waarin deze plichten zijn opgenomen.

8.4 De verwerker mag de persoonsgegevens uitsluitend verwerken in Nederland. Doorgifte naar andere landen is uitsluitend toegestaan na voorafgaande schriftelijke toestemming van de verwerkingsverantwoordelijke en met inachtneming van de toepasselijke wet- en regelgeving.

8.5 De verwerker houdt een actueel register bij van de door hem ingeschakelde derden en onderaannemers waarin de identiteit, vestigingsplaats en een beschrijving van de werkzaamheden van de derden of onderaannemers zijn opgenomen, alsmede eventuele door de verwerkingsverantwoordelijke gestelde aanvullende voorwaarden.

**Artikel 9 Wijziging en beëindigen verwerkersovereenkomst**

9.1 Wijziging van deze verwerkersovereenkomst kan slechts schriftelijk plaatsvinden middels een door beide partijen geaccordeerd voorstel.

9.2 Zodra de samenwerking is beëindigd, zal de verwerker naar keuze van de verwerkingsverantwoordelijke (i) alle of een door verwerkingsverantwoordelijke bepaald gedeelte van haar in het kader van deze verwerkersovereenkomst ter beschikking gestelde persoonsgegevens aan de verwerkingsverantwoordelijke ter beschikking stellen (ii) de persoonsgegevens die hij van de verwerkingsverantwoordelijke heeft ontvangen op alle locaties vernietigen, in welke vorm dan ook en toont dit aan, tenzij partijen iets anders overeenkomen. De verantwoordelijk kan zo nodig nadere eisen stellen aan de wijze van beschikbaarstelling, waaronder eisen aan het bestandsformaat, dan wel vernietiging. Deze werkzaamheden moeten, binnen nader overeen te komen redelijke termijn, uitgevoerd worden en hiervan wordt een verslag gemaakt.

9.3 De verwerker zal te allen tijde de in het vorig lid beschreven recht op overdraagbaarheid van gegevens conform artikel 20 AVG waarborgen, zodanig dat er geen sprake is van verlies van functionaliteit of (delen van) de gegevens.

9.4 Verwerkingsverantwoordelijke en verwerker treden met elkaar in overleg over wijzigingen in deze verwerkersovereenkomst als een wijziging in regelgeving of een wijziging in de uitleg van regelgeving daartoe aanleiding geven.

9.5 Indien een partij tekortschiet in de nakoming van een overeengekomen verplichting, kan de andere partij haar in gebreke stellen waarbij de nalatige partij alsnog een redelijke termijn voor de nakoming wordt gegund. Blijft nakoming ook dan uit dan is de nalatige partij in verzuim.

Ingebrekestelling is niet nodig wanneer voor de nakoming een fatale termijn geldt, nakoming blijvend onmogelijk is of indien uit een mededeling dan wel de houding van de andere partij moet worden afgeleid dat deze in de nakoming van haar verplichting zal tekortschieten.

9.6 De verwerkingsverantwoordelijke is gerechtigd, onverminderd hetgeen daartoe bepaald is in de verwerkersovereenkomst en de daarmee samenhangende hoofdovereenkomst, en onverminderd hetgeen overigens in de wet is bepaald, de uitvoering van deze verwerkersovereenkomst door middel van een aangetekend schrijven op te schorten, dan wel zonder rechterlijke tussenkomst met onmiddellijke ingang geheel of gedeeltelijk te ontbinden, nadat verwerkingsverantwoordelijke constateert dat:

a) verwerker (voorlopige) surseance van betaling aanvraagt; of
b) verwerker zijn faillissement aanvraagt of in staat van faillissement wordt verklaard; of
c) de onderneming van verwerker wordt ontbonden; of
d) verwerker zijn onderneming staakt; of
e) sprake is van een ingrijpende wijziging in de zeggenschap over de activiteiten van de onderneming van verwerker die maakt dat het in alle redelijkheid niet van de verwerkingsverantwoordelijke kan worden verwacht dat zij de verwerkersovereenkomst in stand houdt; of
f) op een aanmerkelijk deel van het vermogen van verwerker beslag wordt gelegd (anders dan door verantwoordelijke); of

g) de andere partij aantoonbaar tekortschiet in de nakoming van de verplichtingen die voortvloeien uit deze verwerkersovereenkomst en die ernstige toerekenbare tekortkoming niet binnen 30 dagen is hersteld na een daartoe strekkende schriftelijke ingebrekestelling dan wel een van de overige situaties bedoeld in artikel 9.5 zich voordoet.

9.7 Verwerker informeert ogenblikkelijk de verwerkingsverantwoordelijke indien een faillissement dreigt dan wel surseance van betaling, zodat de verwerkingsverantwoordelijke tijdig kan beslissen de persoonsgegevens terug te vorderen alvorens faillissement wordt uitgesproken.

9.8 Verwerkingsverantwoordelijke is gerechtigd deze verwerkersovereenkomst en de hoofdovereenkomst per direct te ontbinden indien verwerker te kennen geeft niet (langer) te kunnen voldoen aan de betrouwbaarheidseisen die op grond van ontwikkelingen in de wet en/of de rechtspraak aan de verwerking van de persoonsgegevens worden gesteld.

9.9 Indien de verwerkersovereenkomst voortijdig wordt beëindigd is artikel 9 lid 2 en 3 van overeenkomstige toepassing.

**Artikel 10 Aansprakelijkheid**

10.1 Indien de verwerker tekortschiet in de nakoming van de verplichting uit deze verwerkersovereenkomst kan verwerkingsverantwoordelijke hem in gebreke stellen. Verwerker is echter onmiddellijk in gebreke als de nakoming van desbetreffende verplichting anders dan door overmacht binnen de overeengekomen termijn, reeds blijvend onmogelijk is. Ingebrekestelling geschiedt schriftelijk, waarbij aan de verwerker een redelijke termijn wordt gegund om alsnog haar verplichtingen na te komen. Deze termijn is een fatale termijn. Indien nakoming binnen deze termijn uitblijft, is verwerker in verzuim.

10.2 Verwerker is aansprakelijk op grond van het bepaalde in artikel 82 AVG, voor schade of nadeel voortvloeiende uit het niet nakomen van deze verwerkersovereenkomst, daaronder begrepen wanneer bij de verwerking niet wordt voldaan aan de specifiek tot verwerkingsgerichte verplichtingen van de AVG, of buiten de rechtmatige instructies van verwerkingsverantwoordelijke is gehandeld.

10.3 Verwerker vrijwaart verwerkingsverantwoordelijke voor schade of nadeel voor zover ontstaan door werkzaamheid van de verwerker.

10.4 Indien verwerker de in artikel 6 lid 1 van deze verwerkersovereenkomst neergelegde verplichting niet of niet-tijdig nakomt en de toezichthouder de verwerkingsverantwoordelijke dientengevolge een bestuurlijke boete oplegt, is verwerker aansprakelijk en zal verwerkingsverantwoordelijke een contractuele boete ter hoogte van hetzelfde bedrag opleggen aan verwerker. Deze boete is niet vatbaar voor verrekening en opschorting en laat de rechten van verwerkingsverantwoordelijken op nakoming en schadevergoeding onverlet.

**Artikel 11 Toepasselijk recht**

11.1 Op deze verwerkersovereenkomst en op alle geschillen die daaruit mogen voortvloeien of daarmee mogen samenhangen, is het Nederlands recht van toepassing.

**Artikel 12 Overige bepalingen**

12.1 Deze verwerkersovereenkomst kan worden aangehaald als 'Verwerkersovereenkomst uitvoering < >'.

12.2 De Afdeling Bedrijfsvoering van de gemeente Lopik treedt namens de verwerkingsverantwoordelijke op als contactpersoon.

12.3 Indien partijen eerder een bewerkers- of verwerkersovereenkomst hebben gesloten, verklaren partijen dat deze eerdere overeenkomst(en) vervallen met het sluiten de huidige verwerkersovereenkomst.

Aldus in tweevoud opgesteld en getekend de dato:

Namens de verwerkingsverantwoordelijke, het hoofd van de afdeling Bedrijfsvoering van de gemeente Lopik:

Namens de <nader in te vullen gegevens verwerker>
<nader in te vullen gegevens vertegenwoordiger verwerker, zoals genoemd in de aanhef>

GEMEENTE LOPIK

**Bijlage A: Beschrijving beveiliging**
Beschrijving beveiliging ter uitwerking van artikel 1 lid 2

1. Normenstelsel (kies a of b)
   a. De informatiebeveiliging vindt plaats volgens algemeen erkende normen, namelijk: (vermeld normenstelsel, zoals bijvoorbeeld NEN7510, NEN/ISO 27001, PCI/DSS)
   b. De informatiebeveiliging vindt plaats volgens een algemeen erkende overheidsnorm zoals de BIG of de BIR of vergelijkbaar.

2. De toereikendheid van de informatiebeveiliging blijkt uit:
   a. Certificering;
   b. Periodieke externe controles zoals audits of TPM's (bijv. ISAE3xxx SOC type II);
   c. Een Assurance rapport met conclusie over de bevindingen van de auditor;
   d. Eigen controles of eigen mededelingen.

3. Uit de certificering of periodieke externe controles of uit de audits of uit de eigen controles blijkt of kan afgeleid worden dat de beveiliging voldoet aan of gelijkwaardig is met de toelichting (bijlage 4) en de daarin omschreven elementen.

LET OP: gemotiveerd afwijken is toegestaan!

GEMEENTE LOPIK

## Bijlage B: Omschrijving werkzaamheden

Omschrijving werkzaamheden ter uitwerking van artikel 3 lid 1

1. De werkzaamheden van de verwerker (de verleende diensten en de bijbehorende verwerking).

Hier een lijstje opnemen met werkzaamheden die veel voorkomen zoals:

- Hosting bestaande uit activiteiten zoals…
- Back-ups maken en restoren
- Applicatiebeheer bestaande uit activiteiten zoals…
- Technisch beheer bestaande uit activiteiten zoals…
- Database beheer bestaande uit activiteiten zoals…
- Helpdesk bestaande uit activiteiten zoals…
- Communicatievoorziening (zoals berichtenverkeer)
- Archiefbeheer
- Vernietiging van gegevensdragers
- Printing, scanning, kopiëren (lease van Multifunctionals)
- Inhoudelijke werkzaamheden die namens de gemeente worden uitgevoerd zoals:
  - Uitgifte parkeervergunningen o
    Voeren salarisadministratie
  - Bijvoorbeeld: uitvoeren bepaalde gemeentelijke taken uit de Jeugdwet, WMO, participatiewet

Indien de werkzaamheden in de hoofdovereenkomst specifiek omschreven zijn, kan dit lijstje achterwege blijven. Of hier verwijzen naar de hoofdovereenkomst. De achtergrond van de beschrijving is dat je voldoende duidelijk maakt wat er beveiligd moet worden. Het is de bedoeling dat de zinnen afgemaakt worden met specifieke omschrijvingen!

2. Omschrijving van de werkzaamheden van de derden (subverwerkers) als deze er zijn, als bedoeld in artikel 8.

Lijstje opnemen met werkzaamheden die veel voorkomen zoals:

- Hosting bestaande uit activiteiten zoals…
- Back-ups maken en restoren
- Applicatiebeheer bestaande uit activiteiten zoals…
- Technisch beheer bestaande uit activiteiten zoals…
- Database beheer bestaande uit activiteiten zoals…
- Helpdesk bestaande uit activiteiten zoals…
- Communicatievoorziening (zoals berichtenverkeer)
- Onderhoud aan multifunctionals

De achtergrond van de beschrijving is dat er voldoende duidelijk gemaakt wordt wat er beveiligd moet worden. Ook hier geldt dat de zinnen afgemaakt worden met specifieke omschrijvingen!

3. Categorieën personen en soorten persoonsgegevens Algemene omschrijving van de categorieën personen waar de gegevens die verwerkt worden betrekking op hebben zoals: personeelsleden, burgers, ingeschrevenen, vergunning aanvragers, voorziening aanvragers (cliënten). Is er bij de verwerkte gegevens sprake van gegevens van gevoelige aard als bedoelt in de beleidsregels datalekken van de AP:
   - Bijzondere persoonsgegevens zoals bedoeld in artikel 9 AVG. Het gaat hierbij om persoonsgegevens over iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, lidmaatschap van een vakvereniging en om strafrechtelijke persoonsgegevens en persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag. Het Burgerservicenummer (BSN) valt ook onder bijzondere persoonsgegevens.
   - Gegevens over de financiële of economische situatie van de betrokkene. Hieronder vallen bijvoorbeeld gegevens over (problematische) schulden, salaris- en betalingsgegevens.
   - (Andere) gegevens die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene. Hieronder vallen bijvoorbeeld gegevens over gokverslaving, prestaties op school of werk of relatieproblemen.

- Gebruikersnamen, wachtwoorden en andere inloggegevens. De mogelijke gevolgen voor betrokkenen hangen af van de verwerkingen en van de persoonsgegevens waar de inloggegevens toegang toe geven. Bij de afweging moet worden betrokken dat veel mensen wachtwoorden hergebruiken voor verschillende verwerkingen.
- Gegevens die kunnen worden misbruikt voor (identiteits)fraude. Het gaat hierbij onder meer om biometrische gegevens, kopieën van identiteitsbewijzen en om het BSN.

Is er sprake van de verwerking van gegevens over kwetsbare groepen zoals:
- minderjarigen;
- mensen die te maken hebben met stalking; • die in een blijf-van-mijn-lijfhuis verblijven.

Voor bepaalde categorieën van betrokkenen:
- kinderen en mensen met een verstandelijke handicap.

GEMEENTE LOPIK

## Bijlage C: Inlichtingen om incidenten te beoordelen

Inlichtingen om incidenten te beoordelen ter uitwerking van art. 6 lid 1 en 5

De verwerker zal alle inlichtingen verschaffen die de verwerkingsverantwoordelijke noodzakelijk acht om het incident te kunnen beoordelen. Daarbij verschaft verwerker in ieder geval de volgende informatie aan de verwerkingsverantwoordelijke:

- wat de (vermeende) oorzaak is van de inbreuk;
- wat het (vooralsnog bekende en/of te verwachten) gevolg is;
- wat de (voorgestelde) oplossing is;
- contactgegevens voor de opvolging van de melding;
- aantal personen waarvan gegevens betrokken zijn bij de inbreuk (indien geen exact aantal bekend is: het minimale en maximale aantal personen waarvan gegevens betrokken zijn bij de inbreuk);
- een omschrijving van de groep personen van wie gegevens betrokken zijn bij de inbreuk;
- het soort of de soorten persoonsgegevens die betrokken zijn bij de inbreuk;
- de datum waarop de inbreuk heeft plaatsgevonden (indien geen exacte datum bekend is: de periode waarbinnen de inbreuk heeft plaatsgevonden);
- de datum en het tijdstip waarop de inbreuk bekend is geworden bij verwerker of bij een door hem ingeschakelde derde of onderaannemer;
- of de gegevens versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk zijn gemaakt voor onbevoegden;
- wat de reeds ondernomen maatregelen zijn om de inbreuk te beëindigen en om de gevolgen van de inbreuk te beperken.

## Bijlage D: Te nemen beveiligingsmaatregelen

De set maatregelen in deze bijlage is gebaseerd op het standaardniveau van de BIG. Als het gaat om een gegevensverzameling die hoger geclassificeerd is of een hogere risico inschatting heeft (bijzondere persoonsgegevens) of er extra maatregelen nodig zijn op basis van specifieke wetgeving, dan dient deze bijlage te worden uitgebreid.

De nadruk ligt op de integriteit en exclusiviteit van de gegevens, beschikbaarheidseisen horen thuis in een SLA.

| **BIG Nummer** | **titel** | **Maatregel verwerker** |
|---|---|---|
| 6.1.5.1 | Geheimhoudings- overeenkomst | Medewerkers die te maken hebben met persoonsinformatie van de verantwoordelijke dienen een geheimhoudingsverklaring te ondertekenen. Hierbij wordt tevens vastgelegd dat na beëindiging van de functie, de betreffende persoon gehouden blijft aan die geheimhouding. |
| 6.1.8.2 | Onafhankelijke beoordeling van informatiebeveiliging | Periodieke beveiligingsaudits (minimaal eens per twee jaar) worden uitgevoerd volgens afspraken met de verantwoordelijke. |
| 6.2.1.7 | Identificatie van risico's die betrekking hebben op externe partijen | Over het naleven van de afspraken wordt jaarlijks gerapporteerd aan de verantwoordelijke. |
| 6.2.3.1 | Beveiliging behandelen in overeenkomsten met een derde partij | Maatregelen uit de bewerkersovereenkomst zijn geïmplementeerd. |
| 7.2.2.1 | Labeling en verwerking van informatie | De bewerker heeft maatregelen genomen zo dat niet geautoriseerden geen kennis kunnen nemen van persoonsgegevens. |
| 8.1.1.2 | Rollen en verantwoordelijkheden | Het personeel van de bewerker of derden moeten kennis hebben van de verantwoordelijkheden ten aanzien van de bewerking van de persoonsgegevens voor de verantwoordelijke. |
| 8.1.2.1 | Screening | Voor personen is een recente Verklaring Omtrent het Gedrag (VOG) vereist met punten die door de verantwoordelijke zijn aangedragen. Tenzij dit centraal in het contract geregeld is. |
| 8.3.3.1 | Blokkering van toegangsrechten | Toegangsrechten van medewerkers van de bewerker worden direct geblokkeerd als geen toegang voor de bewerking van de persoonsgegevens noodzakelijk is. |
| **BIG Nummer** | **titel** | **Maatregel verwerker** |
| 9.1.2.1 | Fysieke toegangsbeveiliging | Toegang tot beveiligde zones of gebouwen waar persoonsgegevens van de verantwoordelijke zich bevinden is alleen mogelijk na autorisatie daartoe. |
| 9.1.3.1 | Beveiliging van kantoren, ruimten en faciliteiten | Papieren documenten en mobiele gegevensdragers die persoonsgegevens of andere vertrouwelijke gegevens van de verantwoordelijke bevatten worden beveiligd opgeslagen. |
| 10.3.1.1 | Capaciteitsbeheer | De ICT-voorzieningen voldoen aan het voor de dienst overeengekomen niveau van beschikbaarheid. Er worden |

| | | |
|---|---|---|
| | | voorzieningen geïmplementeerd om de beschikbaarheid van componenten te bewaken (bijvoorbeeld de controle op aanwezigheid van een component en metingen die het gebruik van een component vaststellen).<br>Op basis van voorspellingen van het gebruik wordt actie genomen om tijdig de benodigde uitbreiding van capaciteit te bewerkstelligen.<br>Op basis van een risicoanalyse wordt bepaald wat de beschikbaarheidseis van een ICT-voorziening is en wat de impact bij uitval is. Afhankelijk daarvan worden maatregelen bepaald zoals automatisch werkende mechanismen om uitval van (fysieke) ICT-voorzieningen, waaronder verbindingen op te vangen. |
| 10.6.1.2 | Maatregelen voor netwerken | Gegevensuitwisseling tussen vertrouwde en niet vertrouwde zones dient inhoudelijk geautomatiseerd gecontroleerd te worden op aanwezigheid van malware. |
| 10.6.1.3 | Maatregelen voor netwerken | Bij transport van vertrouwelijke informatie over niet vertrouwde netwerken tussen de bewerker en de verantwoordelijke, zoals over het internet, dient altijd geschikte encryptie te worden toegepast. Zie hiertoe 12.3.1.3. |
| 10.6.2.1 | Beveiliging van netwerkdiensten | Beveiligingskenmerken, niveaus van dienstverlening en beheer eisen voor alle netwerkdiensten behoren te worden geïdentificeerd en opgenomen in elke overeenkomst voor netwerkdiensten, zowel voor diensten die intern worden geleverd als voor uitbestede diensten door een bewerker. |
| 10.8.2.2 | Uitwisselingsovereenkomsten | Verantwoordelijkheid en aansprakelijkheid in het geval van informatiebeveiligingsincidenten zijn beschreven, evenals procedures over melding van incidenten van de bewerker naar de verantwoordelijke. |
| 10.8.3.1 | Fysieke media die worden getransporteerd | De bewerker neemt maatregelen om vertrouwelijke informatie te beschermen, zoals:<br>• Versleuteling.<br>• Bescherming door fysieke maatregelen, zoals afgesloten containers.<br>• Gebruik van verpakkingsmateriaal waaraan te zien is of getracht is het te openen • Persoonlijke aflevering.<br>• Opsplitsing van zendingen in meerdere delen en eventueel verzending via verschillende routes. |
| **BIG Nummer** | **titel** | **Maatregel verwerker** |
| 10.10.1.1 | Aanmaken auditlogbestanden | Door de bewerker worden rapportages van logbestanden gemaakt die periodiek worden beoordeeld. Deze periode dient te worden gerelateerd aan de mogelijkheid |

| | | |
|---|---|---|
| | | van misbruik en de schade die kan optreden. |
| 10.10.1.2 | Aanmaken auditlogbestanden | Een logregel bevat minimaal:<br>• Een tot een natuurlijk persoon herleidbare gebruikersnaam of ID.<br>• De gebeurtenis (zie 10.10.2.1).<br>• Waar mogelijk de identiteit van het werkstation of de locatie.<br>• Het object waarop de handeling werd uitgevoerd.<br>• Het resultaat van de handeling.<br>• De datum en het tijdstip van de gebeurtenis. |
| 10.10.1.3 | Aanmaken auditlogbestanden | In een logregel wordt in geen geval gevoelige gegevens opgenomen. Dit betreft onder meer gegevens waarmee de beveiliging doorbroken kan worden (zoals wachtwoorden, inbelnummers, et cetera). |
| 10.10.2.1 | Controle van systeemgebruik | De volgende gebeurtenissen worden in ieder geval opgenomen in de logging:<br>• Gebruik van technische beheerfuncties, zoals het wijzigingen van configuratie of instelling: uitvoeren van een systeemcommando, starten en stoppen, uitvoering van een back-up of restore. • Gebruik van functioneel beheerfuncties, zoals het wijzigingen van configuratie en instellingen, release van nieuwe functionaliteit, ingrepen in gegevenssets (waaronder databases).<br>• Handelingen van beveiligingsbeheer, zoals het opvoeren en afvoeren gebruikers, toekennen en intrekken van rechten, wachtwoord reset, uitgifte en intrekken van cryptosleutels.<br>• Beveiligingsincidenten (zoals de aanwezigheid van malware, testen op vulnerabilities, foutieve inlogpogingen, overschrijding van autorisatiebevoegdheden, geweigerde pogingen om toegang te krijgen, het gebruik van niet operationele systeemservices, het starten en stoppen van security services).<br>• Verstoringen in het productieproces (zoals het vollopen van queues, systeemfouten, afbreken tijdens executie van programmatuur, het niet beschikbaar zijn van aangeroepen programmaonderdelen of systemen).<br>• Handelingen van gebruikers, zoals goede en foute inlogpogingen, systeemtoegang, gebruik van online transacties en toegang tot bestanden door systeembeheerders. |

| | | |
|---|---|---|
| 10.10.3.3 | Bescherming van informatie in logestanden | Logbestanden worden zodanig beschermd dat deze niet aangepast of gemanipuleerd kunnen worden. |
| 10.10.3.5 | Bescherming van informatie in logestanden | De beschikbaarheid van loginformatie is gewaarborgd binnen de termijn waarin loganalyse noodzakelijk wordt geacht, met een minimum van drie maanden, conform de wensen van de verantwoordelijke. Bij een (vermoed) informatiebeveiligingsincident is de bewaartermijn minimaal drie jaar. |
| **BIG Nummer** | **titel** | **Maatregel verwerker** |
| 10.10.6.1 | Synchronisatie van systeemklokken | Er worden maatregelen genomen om er voor te zorgen dat de logbestanden die verzameld worden aan elkaar te relateren zijn, op basis van het tijdstip waarin ze zijn opgetreden. |
| 11.4.2.1 | Authenticatie van gebruikers bij externe verbindingen. | Als externe toegang nodig is tot de persoonsgegevens van de verantwoordelijke door eigen personeel, of personeel van de bewerker, dienen geschikte authenticatie methodes te worden gebruikt. |
| 11.4.5.5 | Scheiding van netwerken | Zonering wordt ingericht met voorzieningen waarvan de functionaliteit is beperkt tot het strikt noodzakelijke (hardening van voorzieningen). |
| 11.5.1.1 | Beveiligde inlogprocedures | Toegang tot de persoonsgegevens van de verantwoordelijke wordt verleend op basis van twee-factor authenticatie. |
| 11.5.1.2 | Beveiligde inlogprocedures | Het wachtwoord wordt niet getoond op het scherm tijdens het ingeven. Er wordt geen informatie getoond die herleidbaar is tot de authenticatiegegevens. |
| 11.5.1.3 | Beveiligde inlogprocedures | Voorafgaand aan het aanmelden wordt aan de gebruiker een melding getoond dat alleen geautoriseerd gebruik is toegestaan voor expliciet door de organisatie vastgestelde doeleinden. |
| 11.5.1.4 | Beveiligde inlogprocedures | Bij een succesvol loginproces wordt de datum en tijd van de voorgaande login of loginpoging getoond. Deze informatie kan de gebruiker enige informatie verschaffen over de authenticiteit en/of misbruik van het systeem. |
| 11.5.1.5 | Beveiligde inlogprocedures | Nadat voor een gebruikersnaam 3 keer een foutief wachtwoord gegeven is, wordt het account minimaal 10 minuten geblokkeerd. Indien er geen lock-out periode ingesteld kan worden, dan wordt het account geblokkeerd totdat de gebruiker verzoekt deze lockout op te heffen of het wachtwoord te resetten. |
| 11.5.2.1 | Gebruikersidentificatie en authenticatie | Bij uitgifte van authenticatiemiddelen wordt minimaal de identiteit vastgesteld, evenals het feit dat de gebruiker recht heeft op het authenticatiemiddel. |
| 11.5.3.1 | Systemen voor wachtwoordbeheer | Er wordt automatisch gecontroleerd op goed gebruik van wachtwoorden (onder andere voldoende sterke wachtwoorden, |

| | | |
|---|---|---|
| | | regelmatige wijziging, directe wijziging van initieel wachtwoord). |
| 11.5.5.1 | Time-out van sessies | De periode van inactiviteit van een werkstation is vastgesteld op maximaal 15 minuten. Daarna wordt de PC vergrendeld. Bij remote desktop sessies geldt dat na maximaal 15 minuten inactiviteit de sessie verbroken wordt. |
| 11.5.6.1 | Beperking van verbindingstijd | De toegang voor onderhoud op afstand door een leverancier wordt alleen opengesteld op basis van een wijzigingsverzoek of storingsmelding, met 2-factor authenticatie en tunneling. |
| 11.6.1.1 | Beperking van toegang tot informatie | In de soort toegangsregels wordt ten minste onderscheid gemaakt tussen lees- en schrijfbevoegdheden. |
| **BIG Nummer** | **titel** | **Maatregel verwerker** |
| 11.6.1.2 | Beperking van toegang tot informatie | Managementsoftware heeft de mogelijkheid gebruikerssessies af te sluiten. |
| 11.6.1.3 | Beperking van toegang tot informatie | Bij extern gebruik vanuit een niet vertrouwde omgeving vindt sterke authenticatie (two-factor) van gebruikers plaats. |
| 12.1.1.1 | Analyse en specificatie van beveiligingseisen | In projecten ten behoeve van systemen voor de verantwoordelijke wordt een beveiligingsrisicoanalyse en maatregelbepaling opgenomen als onderdeel van het ontwerp. Ook bij wijzigingen worden de veiligheidsconsequenties meegenomen. |
| 12.2.1.1 | Validatie van invoergegevens | Er moeten controles worden uitgevoerd op de invoer van gegevens. Daarbij wordt minimaal gecontroleerd op grenswaarden, ongeldige tekens, onvolledige gegevens, gegevens die niet aan het juiste format voldoen, toevoegen van parameters (SQL-Injectie) en inconsistentie van gegevens. |
| 12.2.2.1 | Beheersing van interne gegevensverwerking | Er bestaan voldoende mogelijkheden om reeds ingevoerde gegevens te kunnen corrigeren door er gegevens aan te kunnen toevoegen. |
| 12.2.3.1 | Integriteit van berichten | Er behoren eisen en geschikte beheersmaatregelen te worden vastgesteld en geïmplementeerd, voor het bewerkstelligen van authenticiteit en het beschermen van integriteit van berichten in toepassingen. |
| 12.2.4.1 | Validatie van uitvoergegevens | De uitvoerfuncties van programma's maken het mogelijk om de volledigheid en juistheid van de gegevens te kunnen vaststellen (bijvoorbeeld door check-sums). |
| 12.3.1.1 | Beleid voor het gebruik van cryptografische beheersmaatregelen | De gebruikte cryptografische algoritmen voor versleuteling zijn als open standaard gedocumenteerd en zijn door onafhankelijke betrouwbare deskundigen getoetst. |

| | | |
|---|---|---|
| 12.3.2.1 | Sleutelbeheer | In het sleutelbeheer is minimaal aandacht besteed aan het proces, de actoren en hun verantwoordelijkheden. |
| 12.4.1.1 | Beheersing van operationele software | Alleen geautoriseerd personeel kan functies en software installeren of activeren. |
| 12.5.1.1 | Procedures voor wijzigingsbeheer | Er is aantoonbaar wijzigingsmanagement ingericht volgens gangbare best practices, zoals ITIL en voor applicaties ASL. |
| 12.5.2.1 | Technische beoordeling van toepassingen na wijzigingen in het besturingssysteem | Van aanpassingen (zoals updates) aan softwarematige componenten van de technische infrastructuur wordt vastgesteld dat deze de juiste werking van de technische componenten niet in gevaar brengen en de beveiliging zoals afgesproken met de verantwoordelijke te niet doen. |
| 12.5.4.1 | Uitlekken van informatie | Op het grensvlak van een vertrouwde en een niet vertrouwde omgeving vindt content-scanning plaats. |
| 12.5.4.2 | Uitlekken van informatie | Er dient een proces te zijn om aan de verantwoordelijke te melden dat (persoons) informatie is uitgelekt. (zie 13.1.1) |
| **BIG Nummer** | **titel** | **Maatregel verwerker** |
| 12.6.1.1 | Beheersing van technische kwetsbaarheden | Er is een proces ingericht voor het beheer van technische kwetsbaarheden. Dit omvat minimaal het melden van incidenten aan de verantwoordelijke, het uitvoeren van periodieke penetratietests, het uitvoeren van risicoanalyses van kwetsbaarheden en patching van systemen en hardware. |
| 13.1.1.1 | Rapportage van informatiebeveiligingsgebeurtenissen | Er is een procedure voor het rapporteren van beveiligingsgebeurtenissen aan de verantwoordelijke vastgesteld, in combinatie met een reactie- en escalatieprocedure voor incidenten, waarin de handelingen worden vastgelegd die moeten worden genomen na het ontvangen van een rapport van een beveiligingsincident. |
| 13.1.1.4 | Rapportage van informatiebeveiligingsgebeurtenissen | Alle beveiligingsincidenten worden vastgelegd in een systeem en geëscaleerd aan de verantwoordelijke. |
| 13.1.1.5 | Rapportage van informatiebeveiligingsgebeurtenissen | Vermissing of diefstal van apparatuur of media die gegevens van de verantwoordelijke kunnen bevatten wordt altijd ook aangemerkt als informatiebeveiligingsincident. |
| 13.2.3.1 | Verzamelen van bewijsmateriaal | Voor een vervolgprocedure naar aanleiding van een beveiligingsincident behoort bewijsmateriaal te worden verzameld, bewaard en gepresenteerd in overeenstemming met de voorschriften voor bewijs die voor het relevante rechtsgebied zijn vastgelegd. |
| 15.1.3.1 | Bescherming van bedrijfsdocumenten | De registraties van de verantwoordelijke behoren te worden beschermd tegen |

| | | |
|---|---|---|
| | | verlies, vernietiging en vervalsing, in overeenstemming met wettelijke en regelgevende eisen, contractuele verplichtingen en bedrijfsmatige eisen. |
| 15.1.4.1 | Bescherming van gegevens en geheimhouding van persoonsgegevens | De bescherming van gegevens en privacy behoort te worden bewerkstelligd in overeenstemming met relevante wetgeving, voorschriften en indien van toepassing contractuele bepalingen. |
| 15.1.6.1 | Voorschriften voor het gebruik van cryptografische beheersmaatregelen | Er is vastgesteld aan welke overeenkomsten, wetten en voorschriften de toepassing van cryptografische technieken moet voldoen. Zie ook 12.3. |
| 15.2.1.1 | Naleving van beveiligingsbeleid en -normen | De bewerker is verantwoordelijk voor uitvoering en beveiligingsprocedures en toetsing daarop (onder andere de jaarlijkse in control verklaring). Conform deze bewerkersovereenkomst en andere contractuele eisen zorgt de bewerker voor het toezicht op de uitvoering van het beveiligingsbeleid ten behoeve van de gegevens van de verantwoordelijke. Daarbij behoren ook periodieke beveiligingsaudits. Deze kunnen worden uitgevoerd door, of vanwege de verantwoordelijke. |
| 15.2.2.1 | Controle op technische naleving | Informatiesystemen van de bewerker ten behoeve van de verantwoordelijke worden regelmatig gecontroleerd op naleving van beveiligingsnormen. Dit kan door bijvoorbeeld kwetsbaarheidsanalyses en penetratietesten. |

GEMEENTE LOPIK

**Bijlage 2 Protocol gegevensverstrekking verwerkingsverantwoordelijke/ gemeente**
Voor de uitvoering van taken kan de gemeente voor verwerking van persoonsgegevens samenwerking aan gaan met andere verwerkingsverantwoordelijken. Binnen de samenwerkingsrelatie blijven alle betrokken verwerkingsverantwoordelijken zelfstandig verantwoordelijk voor de 'eigen' verwerkingen.

Dit protocol voorziet in de verstrekking van persoonsgegevens door de gemeente aan de samenwerkingsrelatie om een gezamenlijk doel te bereiken voor zover deze persoonsgegevens noodzakelijk zijn voor de uitvoering van de taken van de desbetreffende samenwerkingsverband. Met inachtneming van het bij of krachtens de Algemene Verordening Gegevensbescherming (AVG) bepaalde geschiedt het verstrekken van persoonsgegevens overeenkomstig dit protocol.

Dit protocol gegevensverstrekking is geldend vanaf ..... en wordt voorafgaande aan elke eerste verstrekking voor een bepaald doel aan de partners in het samenwerkingsverband gezonden.

**Protocol**

1. In gevallen waarin de samenwerkingspartner(s) persoonsgegevens willen ontvangen van de gemeente ter uitoefening van hun taken in de samenwerkingsafspraken, dien(t)en zij een daartoe strekkend verzoek in bij de desbetreffende gemeente. In het verzoek worden de volgende onderwerpen beschreven:
   - Doel en grondslag van de verwerking,
   - Aantonen of contractspartij verwerkingsverantwoordelijke is,
   - Welke persoonsgegevens men van de gemeente wenst te ontvangen,
   - Welke passende technische en organisatorische maatregelen de contractspartij heeft genomen om persoonsgegevens te verwerken,
   - - Welke maatregelen zijn genomen om verdere onrechtmatige verwerking te voorkomen, - Vanaf welke datum overdracht van persoonsgegevens zal geschieden.

2. Voor de uitvoering van wettelijke taken door de samenwerkingspartner kan de gemeente alle bij haar bekende persoonsgegevens in een concrete situatie of in een verzameling concrete situaties ter verwerking overdragen aan de ander onder de restrictie dat enkel die persoonsgegevens worden overgedragen waarbij de samenwerkingspartner een aanwijsbaar belang heeft ten behoeve van de uitvoering van diens wettelijke taken.

3. Indien door de contractspartner geen wettelijke taak wordt uitgevoerd kan de gemeente alle bij haar bekende persoonsgegevens in een concrete situatie ter verwerking overdragen aan de samenwerkingspartner, indien noodzakelijk ter bescherming van een vitaal belang van de betrokkene of diens naasten onder de restrictie dat enkel die persoonsgegevens worden overgedragen waarbij de samenwerkingspartner een aanwijsbaar belang heeft ten behoeve van de uitvoering van diens werkzaamheden. Indien de wettelijke grondslag en het vitaal belang ontbreken is overdracht van persoonsgegevens enkel mogelijk met uitdrukkelijke toestemming van de betrokkene.

4. De persoonsgegevens die op grond van artikel 2 en 3 van de gemeente worden ontvangen zullen door de contractspartners worden verwerkt met inachtneming van de wettelijke voorschriften, waaronder de AVG, in welk kader de samenwerkingspartners voorafgaand aan de eerste verstrekking een privacy beleid zullen opstellen dat in overeenstemming is met dit protocol. Een exemplaar van dit beleidsplan zal aan de gemeente ter hand worden gesteld.

5. Voor de uitvoering van de verwerking door de contractspartners die geen verwerkingsverantwoordelijke zijn zal tussen gemeente en de contractspartner een overeenkomst als bedoeld in artikel 28 lid 3 AVG en/of artikel 7 Besluit basisregistratie personen worden opgesteld.

6. Contractspartners zullen de gemeente onmiddellijk op de hoogte stellen van een datalek als bedoeld in artikel 33 AVG, alle noodzakelijke maatregelen nemen om het lekken te doen stoppen en om alle informatie en medewerking te verlenen waar de gemeente om verzoekt.

7. Samenwerkingspartners zullen de van de gemeente verkregen persoonsgegevens niet verder verwerken op een wijze die onverenigbaar is met de doeleinden waarvoor de persoonsgegevens

zijn verkregen. Samenwerkingspartners zullen de persoonsgegevens niet openbaren of aan derden verstrekken, behoudens voor zover daartoe een wettelijke verplichting bestaat. Verdere verwerking van de persoonsgegevens voor statistische of wetenschappelijk doeleinden wordt niet als onverenigbaar beschouwd, indien de nodige voorzieningen zijn getroffen ten einde te verzekeren dat de verdere verwerking uitsluitend geschiedt ten behoeve van deze specifieke doeleinden.

8. Overdracht van de aansprakelijkheid voor onrechtmatige verwerkingen geschiedt op het moment dat de gemeente voor de eerste maal persoonsgegevens overdraagt aan de samenwerkingspartner.

GEMEENTE LOPIK

**Bijlage 3 Geheimhoudingsverklaring**
De gemeente hecht waarde aan een goede naleving van de privacywetgeving. Door ondertekening van deze privacyverklaring kunnen persoonsgegevens die door u in het kader van de uitoefening van gemeentelijke taken worden verwerkt met u worden gedeeld..

De ondergetekende:

Naam: ……..

Verklaart en gaat er mee akkoord dat:

Artikel 1.
Het college van burgemeester en wethouders stemt erin toe dat u voor de uitvoering van uw taken persoonsgegevens, waarvoor de gemeente verwerkingsverantwoordelijke of verwerker is, verwerkt, tenzij enige wettelijke bepaling aan het inzien van deze persoonsgegevens in de weg staat.

Artikel 2
Het is niet toegestaan om persoonsgegevens die u verwerkt met anderen, zowel binnen als buiten de gemeentelijke organisatie te delen, tenzij het delen een noodzakelijk uitvloeisel is van de opgedragen taken. Bij het delen van persoonsgegevens worden de wettelijke plichten en de richtlijnen van de gemeente in acht genomen.

Artikel 3
Na afronding van uw taken bij de gemeente blijft de geheimhoudingsverklaring van kracht.

Aldus getekend op ……..

……..

GEMEENTE LOPIK

## Bijlage 4 Activiteitenoverzicht

Na vaststelling van het beleidsplan privacy worden een aantal activiteiten opgepakt ter verdere uitwerking van het beleidsplan. In het schema staan de verschillende activiteiten opgesomd, onder wiens verantwoordelijkheid de activiteit valt, naar welke aanbeveling in het rapport van A3P (juni 2018) de activiteit verwijst, het aantal uren noodzakelijk voor uitvoering met daarbij de vraag of het om een incidentele of structurele activiteit gaat en tot slot de planning.

Activiteit Verantwoordelijkheid Hfs uit BP Concl.A3P In uitvoering Inc of Struct Gereed

| | | | | | | |
|---|---|---|---|---|---|---|
| Projectleider implementatie onderstaande | Privacy officer | | | | I | Q4 2018 en Q1 2019 |
| activiteiten | | | | | | |
| Toedeling thema privacy aan portefeuillehouder | College | 5 | | | I | Q4 2018 |
| Mandaatbesluit ondertekening verwerkersovereenkomst en protocollen | College | 5 | | Ja, mandaat ligt bij Mgr bedrijfsvoering | I | Q4 2018 |
| Werkinstructies opstellen voor:<br>- Uitvoeren rechten van betrokkenen (Art 15 ev. AVG)<br>- Behandelen bezwaren van betrokkenen (Art 21 AVG) | Privacy officer/FG | 6 | 12,2 | Ja | I | Q4 2018 |
| Werkinstructies opstellen voor:<br>- Veilig delen van persoonsgegev ens (mn. Triages)<br>- Opslaan persoonsgegevens in archieven<br>- Cameratoezicht<br>- Gebruik BSN<br>- Datalekken<br>- Omgaan met ID-bewijzen<br>- GEO-viewer en Cyclorama<br>- Beheer van devices | Privacy officer/FG | 7 | 3, 6, 8, 9, 10, 12, 14, 15, 16, 17, 18, 19, 20 | Ja | I | Q4 2018 |
| Aanschaf beveiligde devices voor gebruik buitenshuis, inrichten en instrueren | CISO | 7 | | Ja, nog geen staand beleid | I | Q1 2019 |
| Integratie van privacy- en veiligheidsbeleid in de jaarlijkse planning en controlcyclus | Controller | 7 | 1 | Ja, wordt tzt meegenomen | I | Q1 2019 |
| Inrichten risk-based toezichtsmodel (mede aan de hand van PIA's) | Functionaris gegevensbescherming | 5 | | Ja | I | Q1 2019 |
| Opstellen communicatieschema | Communicatiemanager | 8 | 11 | Nee | S | |

| | | | | | | |
|---|---|---|---|---|---|---|
| bewust omgaan met persoonsgegevens (intern en extern) | | | | | | |
| Uitvoeren PIA's en trainen medewerkers | Functionaris gegevensbescherming | 5 | | Nee | S | |
| Inrichting van het privacy-platform (driehoek), inclusief centraal communicatiemiddel, en aanstellen van medewerkers | Privacy officer, CISO en FG | 5 | 2 | Nee | S | |
| Passende technische maatregelen voor veilig gebruik persoonsgegevens conform artikel 25 AVG | CISO | 9 | | Ja op organisatieniveau en Nee op werkprocesniveau | S | |
| Contractmanagement voor verwerkingsovereenkomsten en | Privacy officer | 4 | 4,13 | Nee | S | |
| Vaststellen takenpakket medewerkers en toegang tot bestanden | Afdelingsmanagers | 7 | 5, 7 | Nee | S | |
| Opstellen jaarlijks activiteitenplan bewust omgaan met persoonsgegevens | Afdelingsmanagers | 8 | 13 | Nee | S | |

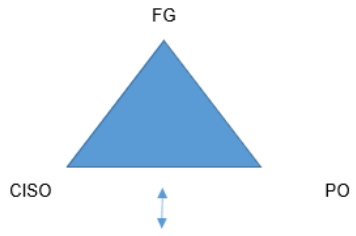
Voor de inrichting van de verantwoordelijkheden en het verdelen van de taken wordt sterk gekeken naar het schema op bladzijde 13 van het beleidsplan.

Bestuurlijk niveau Wethouder (portefeuillehouder privacy)

Bestuurlijke
verantwoordelijkheid

Bedrijfsvoeringsniveau Manager bedrijfsvoering

Ambtelijk opdrachtgever




Afdelingsniveau Afdelingsmanagers

medewerkers
In deze setting berust de uitvoering bij, primair, de privacy officer en de CISO. Voor het beschrijven van taken medewerkers (en de toegang die daaruit voortvloeit voor de bestanden) wordt een inbreng gevraagd van de afdelingsmanagers en de medewerkers.

Naar verwachting kunnen de nog openstaande activiteiten met de huidige bezetting worden uitgevoerd. Dit betekent dat er momenteel geen behoefte bestaat de gemeenteraad te vragen een besluit te nemen over aanvullende middelen. Het beleidsplan wordt wel ter kennisneming naar de gemeenteraad gestuurd.

GEMEENTE LOPIK

Na vaststelling van het beleidsplan privacy wordt het plan breed gecommuniceerd en wordt voor medewerkers een cursus georganiseerd waarbij deelname verplicht is.