Gemeente IJsselstein

# GEMEENTEBLAD

Officiële uitgave van de gemeente IJsselstein

Nr. 424969

22 september 2022

## Beleidsplan veilig omgaan met persoonsgegevens in de gemeente IJsselstein

### 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 (welke is afgeleid van de Europese databeschermingsrichtlijn uit 1995) is een eerste poging ondernomen 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 cloud-toepassingen 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 zullen verwerkingsverantwoordelijken (waaronder gemeenten) vanaf 25 mei 2018 aan de Verordening moeten voldoen. De Wet bescherming persoonsgegevens zal deels worden overgeheveld naar de Uitvoeringswet Algemene Verordening Gegevensbescherming en voor het overige worden ingetrokken.

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

Voldoen aan de AVG betekent dat op verschillende terreinen binnen de gemeentelijke organisatie aandacht moet zijn voor privacy. 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 zullen governance, beleid, werkprocessen en triages, bewustwording en het beheer en opslag van gegevens onder de loep genomen worden die mogelijk leiden tot aanpassing van processen

of werkafspraken. In dit beleidsplan zijn tevens de aanbevelingen uit het rekenkameronderzoek meegenomen.


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

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 is er wel een gemeenschappelijke lijn te ontdekken. De aanbevelingen die uit de verschillende rapportages zijn gekomen, zijn meegenomen in dit beleidsplan en zullen ter uitwerking van dit plan in werkinstructies worden opgenomen. Zie voor het overzicht van activiteiten die uitgevoerd moeten worden na vaststelling van het beleidsplan bijlage 4.

## 2. Collegesamenvatting

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

Waar het gaat om het beschermen van persoonsgegevens geeft de AVG duidelijk richting aan. Persoonsgegevens mogen slechts verwerkt worden indien 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 het grote aantallen gegevensbestanden dat in dat licht verwerkt wordt, zijn er veel doelen aan te wijzen waarvoor gemeenten persoonsgegevens verwerkt. Randvoorwaarde hierbij is wel dat bij de bepaling van het doel nagedacht moet worden over bv 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 teamleiders. Op bedrijfsniveau bieden de functionaris gegevensbescherming, de coördinator informatieveiligheid en de juridisch privacy-adviseur ondersteuning bij het inrichten van de kaders, zijn adviseurs voor technische en organisatorische kwesties, hebben een coördinerende rol in de bedrijfsvoeringscyclus en verwerken datalekken.

De ruimte voor zelfstandige beleid is beperkt. Belangrijke beleidsthema's die spelen zijn in H6 van dit beleidsplan nader uitgewerkt. De gekozen beleidsoplossingen vloeien voort uit de AVG, afzonderlijke materiewetten of jurisprudentie.

Waar het gaat om bedrijfsprocessen, genoemd in H7, wordt aansluiting gezocht bij een belangrijk uitgangspunt van de AVG op dit punt. Enkel voor het uitvoeren van taken hebben medewerkers toegang tot bepaalde bestanden. Om dit mogelijk te maken zal er een autorisatieschema worden opgesteld voor toegang en zal nagedacht worden over het tijdig toelaten en afsluiten van medewerkers tot die bestanden.

Bewust omgaan met persoonsgegevens zal binnen de organisatie een vast thema worden. Aan de hand van verschillende leer- en communicatiemiddelen zullen medewerkers worden meegenomen om be-

wuster met de privacy van betrokkenen om te gaan. Naar verwachting zal de communicatie over bescherming persoonsgegevens gecombineerd worden met informatieveiligheid in zijn algemeenheid.

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 privacy-wetgeving. Het gaat hierbij om:

- Persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon („de betrokkene"); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een 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;
- Bestand: elk gestructureerd geheel van persoonsgegevens die volgens bepaalde criteria toegankelijk zijn, ongeacht of dit geheel gecentraliseerd of gedecentraliseerd is dan wel op functionele of geografische gronden is verspreid;
- Ontvanger: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, al dan niet een derde, aan wie/waaraan de persoonsgegevens worden verstrekt. Overheidsinstanties die mogelijk persoonsgegevens ontvangen in het kader van een bijzonder onderzoek overeenkomstig het Unierecht of het lidstatelijke recht gelden echter niet als ontvangers; de verwerking van die gegevens door die overheidsinstanties strookt met de gegevensbeschermingsregels die op het betreffende verwerkingsdoel van toepassing zijn;
- Derde: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, niet zijnde de betrokkene, noch de verwerkingsverantwoordelijke, noch de verwerker, noch de personen die onder rechtstreeks gezag van de verwerkingsverantwoordelijke of de verwerker gemachtigd zijn om de persoonsgegevens te verwerken;
- Toestemming van de betrokkene: elke vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee de betrokkene door middel van een verklaring of een ondubbelzinnige actieve handeling hem betreffende verwerking van persoonsgegevens aanvaardt;

## 4. Algemeen kader voor de verwerking van persoonsgegevens

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

### 4.1. Doelbinding

Uitgangspunt in de AVG is de verwerking van de persoonsgegevens. Deze verwerkingen worden gedaan in het kader van de taakuitoefening door medewerkers. Voor deze verwerkingen geldt dat er een doel geformuleerd moet worden waarvoor zij worden verwerkt.
De AVG laat in het midden hoe die doelen geformuleerd worden, Uitgangspunt van de verordening is dat persoonsgegevens voor een welbepaald, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld. Het is een simpele aanpak om per afdeling te laten vaststellen voor welke doelen persoonsgegevens worden verwerkt bv vergunningverlening, subsidievaststelling of bepalen 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 is daarbij 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.

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


### 4.2. Toereikend, ter zake dienend en niet bovenmatig

Voor al deze afzonderlijke doeleinden dient vervolgens vastgesteld te worden 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 gaat ontstaan. Ter verduidelijking; een winkelier, die een registratie bijhoudt van wanbetalers, zal een ontoereikende verwerking doen als deze niet tevens registreert of de betaling is opgeschort, omdat de klant een dispuut heeft over het product.
Ter zake dienend hangt nauw samen met het doel. Is het bijhouden door de winkelier bedoeld voor de administratie, dan kunnen de gegevens niet aangewend worden om het koopgedrag te analyseren. Bovenmatig tot slot hangt ook samen met het doel. Houdt de winkelier een registratie bij van wanbetalers voor zijn administratie, dan zal het registeren van de waarde niet bovenmatig zijn, het bijhouden van het aantal goederen mogelijk wel.

Op afdelingsniveau zal men per verwerking moeten vaststellen 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 de persoonlijke levenssfeer van de betrokkenen. Ingevolge het subsidiariteitsbeginsel mag het doel waarvoor de persoonsgegevens worden verwerkt in redelijkheid niet op een andere, voor de bij de verwerking van persoonsgegevens betrokkene, minder nadelige wijze kunnen worden verwerkelijkt (bv het verkrijgen van de informatie uit open data).

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

### 4.4. Grondslag

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

- 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 enkel 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 IJsselstein zal dit in de regel het uitvoeren van wettelijke taken of een goede vervulling van publieke taken zijn) het mogelijk is gegevens te verzamelen, dan wordt geen toestemming aan de betrokkene gevraagd, tenzij een wettelijke bepaling daartoe verplicht.

### 4.5. Verwerkingsverantwoordelijke(n) en verwerker

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

In de relatie verwerkingsverantwoordelijke en verwerker heeft laatstgenoemde geen zeggenschap over het doel en de middelen van de verwerking. Doel en middelen worden door de verwerkingsverantwoordelijke bepaald. Om te zorgen dat de verwerker zich richt naar de instructies van de verwerkingsverantwoordelijke en kan garanderen aan de verwerkingsverantwoordelijke dat het passende technische en organisatorische maatregelen heeft genomen om de rechten van betrokkenen te beschermen, wordt een verwerkersovereenkomst gesloten. De wetgever laat het in het midden of dit een aparte overeenkomst moet zijn of dat deze geïncorporeerd kan worden in de overeenkomst tot opdracht of samenwerkingsovereenkomst.
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 IJsselstein 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 IJsselstein 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 basis-beveiligingsniveau;
- 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.

### 4.7 Samenvatting

De eerste opdracht in het kader van de bescherming van persoonsgegevens is het bepalen van het aantal en de omvang van de verwerkingen die binnen de verschillende teams plaatsvinden.
Op afdelingsniveau vaststellen:

- De omvang van het aantal verwerkingen in bestanden vastleggen in het verwerkingenregister.
- Op afdelingsniveau bepalen voor welke doelen gegevens worden verwerkt en het takenpakket dat hier uit voortvloeit.
- Op afdelingsniveau bepalen wat de grondslag van de verwerkingen is.
- Op afdelingsniveau bepalen welke gegevens naar soort en omvang noodzakelijk zijn om het takenpakket uit te kunnen oefenen.
- Op afdelingsniveau vaststellen welke taken worden uitbesteed en daar een verwerkersovereenkomst of protocol voor afsluiten.
- Op organisatieniveau bepalen welke passende technische en organisatorische maatregelen genomen moeten worden om compliant te zijn in termen van de AVG.

## 5. Governance

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

### 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 IJsselstein belegd bij een van de wethouders of de burgemeester die als vast aanspreekpunt fungeert voor privacy-issues. In de regel zal dit de wethouder zijn die tevens aanspreekpunt is voor de bedrijfsvoering. Op het beleggen van de verantwoordelijkheid bij één wethouder of de burgemeester gelden twee kleine uitzonderingen. Voor verwerkingen die door de burgemeester worden gedaan (denk aan verwerkingen in het kader van de openbare orde en veiligheid), is de burgemeester verantwoordelijke en voor verwerkingen die door de raad worden gedaan is de raad zelf verantwoordelijk.

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 aldus een beleidsvrijheid. Deze beleidsvrijheid wordt primair op afdelingsniveau ingevuld. Onder omstandigheden kan het college uitdrukkelijk gevraagd worden in te stemmen met een verwerking. Het afwegingskader daarbij is de bescherming privacy burger afgezet tegen een eigen belang van de gemeente, bv veiligheid medewerkers.

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

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

Bedenk 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 IJsselstein is er op gericht om geen persoonsgegevens in openbare stukken op te nemen, tenzij het een bewuste keuze is het wel te doen.

### 5.2 Privacy op ambtelijk niveau

De feitelijke verwerking van persoonsgegevens vindt plaats binnen de ambtelijke organisatie op afdelingsniveau. De uitwerking van de eindverantwoordelijkheid die het college draagt wordt ingevuld op dit niveau. Hier worden het doel en de middelen van de verwerking bepaald zoals gebleken is uit hoofdstuk 4. Het is niet meer dan logisch dat een deel van de bevoegdheden en verantwoordelijkheden op het terrein van de privacy die ligt bij het college gemandateerd wordt naar teamleiders, zodat zij op effectieve wijze privacy in hun dagelijkse processen kunnen incorporeren.

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

De verantwoordelijkheid van de teamleiders op privacygebied 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,
- alloceren 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) en
- melden datalekken en andere incidenten

De teamleiders 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 Lekstroomgemeente (bv. Leden van de bezwarencommissie) of die tijdelijk worden ingehuurd geldt dat zij een geheimhoudingsverklaring moeten tekenen. Het template van de geheimhoudingsverklaring is opgenomen in bijlage 3.

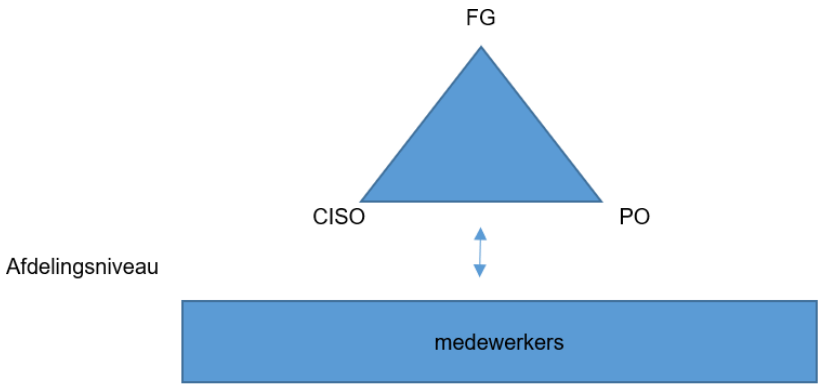
Om de portefeuillehouder betrokken te houden en om, samen met het college, de rol van verwerkingsverantwoordelijke in het kader van de privacy waar te maken zal periodiek een activiteitenoverzicht worden gemaakt. Het is de bedoeling om dit activiteitenoverzicht mee te laten lopen met de bedrijfsvoeringsgesprekken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

### Artikel 5.3 Privacy Office als kader voor informatieveiligheid en privacy-issues

Organisatorisch wordt op twee niveaus uitwerking gegeven aan het privacybeleid; bedrijfsvoerings- en afdelingsniveau. In paragraaf 5.2 is stilgestaan bij de inbedding van privacy op afdelingsniveau. Om voldoende robuustheid te geven aan het privacythema is het wenselijk om daarnaast een aantal rollen binnen de organisatie primair te belasten met privacy waar medewerkers terecht kunnen met vragen op het gebied van privacy en informatieveiligheid. Dit zou (logischerwijs) bij bedrijfsvoering liggen.

Op bedrijfsvoeringsniveau vertaalt het zich in een driehoek bestaande uit Functionaris Gegevensbescherming, Chief information and securityofficer (CISO) en een privacyofficer (PO). Het doel van de driehoek is om 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:




### 5.4 Functionaris Gegevensbescherming (FG)

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

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

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 (Privacy Impact Assessments). 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 de gemeente IJsselstein.

Vanuit de wens van onafhankelijkheid zal de FG formeel geen deel uitmaken van de privacy office. Uiteraard blijft deze functionaris wel nauw betrokken bij de adviezen die door de privacy office gegeven worden

### 5.5 Chief Information security officer (CISO)

De CISO is binnen de gemeentelijke organisatie verantwoordelijk voor het informatiebeveiligingsbeleid en richt met beveiligingsjaarplannen een voortdurende focus op informatieveiligheid dienstbaar aan een goede bedrijfsvoering. In zijn rol ziet hij niet alleen toe op het fysiek beveiligen van gegevens en gebouwen, maar ook op het voorkomen van onrechtmatige inbreuken op de software. Vanuit deze verantwoordelijkheden richt de CISO zich naar de beveiligingseisen die neergelegd zijn in de BIO (baseline informatieveiligheid overheid) en de ENSIA (Eenduidige Normatiek Single Information Audit). Beide kaders liggen vast in ISO-normen en kennen een dwingend voorgeschreven invulling van het veiligheidsbeleid van gemeenten.

Binnen de privacy office heeft de CISO tot taak om alle vragen die te maken hebben met informatieveiligheid te beantwoorden.

### 5.6 Privacy officer (PO)

Binnen de gemeente IJsselstein is de PO verantwoordelijk voor het vormgeven en actualiseren van het gemeentelijke privacy-beleid, het doen van organisatorische aanpassingen en draagt hij zorg 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 de adviseur als aanspreekpunt voor vragen over toepassing wet- en regelgeving inzake privacy.

Nu teamleiders nadrukkelijk verantwoordelijkheid dragen voor de verwerkingen die op hun afdeling wordt 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 hetgeen staat opgesomd in paragraaf 5.2.
Zo zal deze medewerker binnen de afdeling als aanspreekpunt belast worden met de dagelijkse praktijk fungeren en werkinstructies schrijven. Uiteraard kan deze medewerker voor ingewikkelder vraagstukken ondersteuning vragen bij de driehoek.

### 5.6 Externe relaties/verwerkersovereenkomst

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

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

*A gezamenlijke verwerkingsverantwoordelijkheid*

Van een gezamenlijk verwerkingsverantwoordelijkheid is sprake wanneer twee of meer verwerkingsverantwoordelijken gezamenlijk de doeleinden en middelen van de verwerking bepalen. In dat geval stellen zij op transparante wijze hun respectieve verantwoordelijkheden voor de nakoming van hun verplichting uit hoofde van de AVG vast, met name met betrekking tot de uitoefening van rechten van betrokkenen en het verstrekken van informatie aan hen. De relatie tussen de verwerkingsverantwoordelijken onderling wordt bestendigd door middel van een protocol. 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 met betrekking tot het toepassen van passende technische en organisatorische maatregelen bieden 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 zal de gemeente in deze situaties gebruik maken van verwerkersovereenkomsten. Het gebruik van verwerkingsovereenkomsten is een verplichting die voortvloeit uit de AVG. De verwerkingsovereenkomst is vormvrij en kan dus ook geregeld worden 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 zal er na overdracht geen gebondenheid meer zijn van de gemeente IJsselstein. De inspanning van de gemeente IJsselstein 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.

## 6 Privacybeleid

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

andere hulpverleners langs elkaar heen werken. Beslissingen die in dat verband genomen worden zullen duidelijk gemotiveerd worden.

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

Binnen het thema beleid verdienen 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 opdat zij steeds de regie kunnen voeren op de persoonsgegevens die bij de gemeente IJsselstein worden verwerkt.
Het gaat om de volgende rechten:

1. Recht op informatie (artikel 12 AVG)
   Er dienen maatregelen genomen te worden zodat de betrokkene op een beknopte, transparante, begrijpelijke en in gemakkelijk toegankelijke vorm informatie kan verkrijgen over zijn persoonsgegevens en geïnformeerd wordt over verwerkingsactiviteiten.
   Het verstrekken van informatie geschiedt onverwijld en in ieder geval binnen een maand na ontvangst van het verzoek.
   Recht op inzage (artikel 15 AVG)
2. 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 en
   - 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 recificatie 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 zal moeten worden bepaald of gegevenswissing mogelijk is. De verwerkingsverantwoordelijke stelt iedere betrokkene op de hoogte van de wissing.
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 IJsselstein is dat gestreefd wordt naar een maximale transparantie tegenover de betrokkene waar het gaat om de 'eigen' persoonsgegevens.
Waar het gaat om het recht op informatie zullen de gemeenten in zijn algemeenheid op de website en in de correspondentie betrokkenen wijzen 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 privacy officer (zie paragraaf 5.6) 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 raad- 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 welke is toegevoegd aan de agenda. Na afloop van de collegevergadering wordt het inlegvel verwijderd. De verantwoordelijk wethouder of burgemeester (die juist wel 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 zal aan de raad worden aangeboden door de betreffende wethouder of de burgemeester.

In correspondentie naar burgers kan het persoonsgegeven van de medewerker genoemd worden, indien dit noodzakelijk is (bv. welke wmo-consulent gaat uw dossier behandelen). In die gevallen dat er geen noodzaak is persoonsgegevens van medewerkers te delen zal de naam van de medewerker worden vervangen door een alias (bv. 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 d Wob vloeit dit al voort. In het kader van dit beleidsplan wordt artikel voornoemde regel gevolgd met de aanvulling dat er snel sprake zal zijn van een aantasting van de persoonlijke levenssfeer. Voor degene die Wob-verzoeken afhandelt betekent dit een extra alertheid.

### 6.3 Geautomatiseerde verwerkingen en cameratoezicht

Onder geautomatiseerde verwerkingen wordt verstaan het met gebruikmaking van elektronische middelen gegevens verwerken. Een voorbeeld 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 IJsselstein wordt hier geen gebruik van gemaakt.

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

Gemeente IJsselstein maakt op dit moment gebruik cameratoezicht. Waar het gaat om cameratoezicht houden de gemeenten die het aangaan 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 niet langer dan 4 weken worden bewaard en dat er Privacy Impact Assessment (PIA) zal worden uitgevoerd.

Gemeente IJsselstein maakt gebruik van cameratoezicht in de raadszaal. Dit gebruik is toegestaan mits duidelijk wordt aangegeven aan betrokkenen dat cameratoezicht plaatsvindt.

### 6.4 Datalekken

Van een datalek is sprake bij een onrechtmatige verwerking en als persoonsgegevens in handen vallen van derden die geen toegang tot die gegevens zouden mogen hebben. Een datalek is het gevolg van een beveiligingsincident. In de meeste gevallen gaat het om uitgelekte computerbestanden, al kan een verloren uitgeprinte klantenlijst evengoed een datalek vormen. Andere voorbeelden: 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 heeft de gemeente IJsselstein inmiddels een werkinstructie meldplicht datalekken zal dit beleidsthema hier verder onbesproken blijven. (zie bijlage 5)

### 6.5 Bewaren van persoonsgegevens

Persoonsgegevens mogen niet langer worden bewaard dan noodzakelijk is voor de verwerking. Voor wat betreft het bewaren van persoonsgegevens geldt voor de gemeente IJsselstein twee regiems, het wettelijke regiem en het niet wettelijke regiem.
Voor sommige verwerkingen van persoonsgegevens geldt dat deze persoonsgegevens op grond van de Archiefwet of andere materiële wetten een minimale termijn bewaard moeten blijven. Een voorbeeld is het jeugdhulpdossier dat 15 jaar nadat de jeugdhulp beëindigd is bewaard moet blijven. De AVG gaat niet in op de wettelijke termijnen die bestaan of in de toekomst zullen ontstaan.
Voor die verwerkingen waarvoor geen wettelijke termijn geldt, bv. de gemeente heeft een onderzoek gedaan naar relschoppers in de wijk X, dat de verwerkte persoonsgegevens worden vernietigd zodra de verwerking niet meer noodzakelijk is ter bepaling door de afdelingsmanager en wordt vastgelegd in het verwerkingsregister.

Voor wat betreft het archiveren van persoonsgegevens zoekt de gemeente IJsselstein 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 verwerkt mogen worden in de zin van archiveren (verenigbaar doel). Wel zal men opnieuw moeten beoordelen of verdere dataminimalisatie mogelijk is. Is dataminimalisatie mogelijk door ontkoppeling van de persoonsgegevens met de overige gegevens, dan zal daar voor gekozen worden. Als tussenvorm is het mogelijk om in het kader van archivering te werken met pseudonimiseren.

Om Archiveren in goede banen te leiden zal er apart onderzoek worden gedaan naar het opslaan van persoonsgegevens in gemeentelijke archieven. De insteek zal zijn 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 IJsselstein de verwerking van persoonsgegevens vorm geeft in bedrijfsprocessen en op welke wijze medewerkers gebruik kunnen maken van databases. In 7.1 zal het kader geschetst worden 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 dagelijks praktijk. 7.3 gaat dieper in op triages die hoofdzakelijk voorkomen in het sociaal domein. 7.4 bespreekt het gebruik van BSN (een persoonsgegeven ogv Uitvoeringswet AVG). In 7.5 wordt dieper ingegaan op het verwerkingenregister dat door de gemeente moet worden aangelegd en op basis waarvan de FG zijn toezicht kan effectueren. In de laatste paragraaf wordt besproken hoe met Privacy Impact Assessments (PIA's) privacyrisico's van gegevensverwerkingen in beeld gebracht worden en hoe deze vervolgens te vertalen in het werkproces.

### 7.1 Inbedding in primaire processen

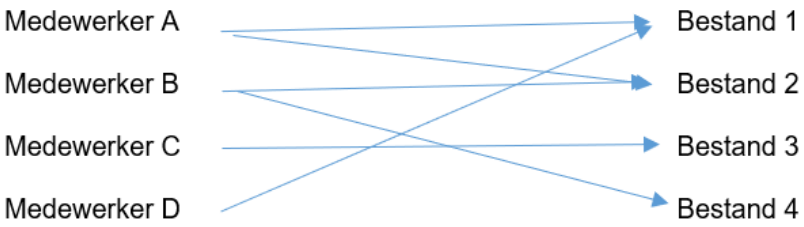
De AVG eist dat voor gemeente IJsselstein verwerking van persoonsgegevens de beginselen inzake verwerking van persoonsgegevens in acht genomen zijn. Deze beginselen vloeien voort uit artikel 5 en 6 AVG (zie voor verdere uitleg H4 van dit beleidsplan).

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

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

De volgende stap is dat aansluiting gevonden wordt bij een van de grondslagen uit artikel 6 AVG (zie tevens paragraaf 4.4). Voor de gemeente IJsselstein zal gaan gelden dat veel verwerkingen als grondslag de goede vervulling van een publieke taak kennen. In bijzondere gevallen zal een beroep op een van de andere grondslagen, ten finale mogelijk toestemming, gedaan moeten worden.

Schematische weergave van verdeling takenpakket en toegang tot gegevensbestanden:



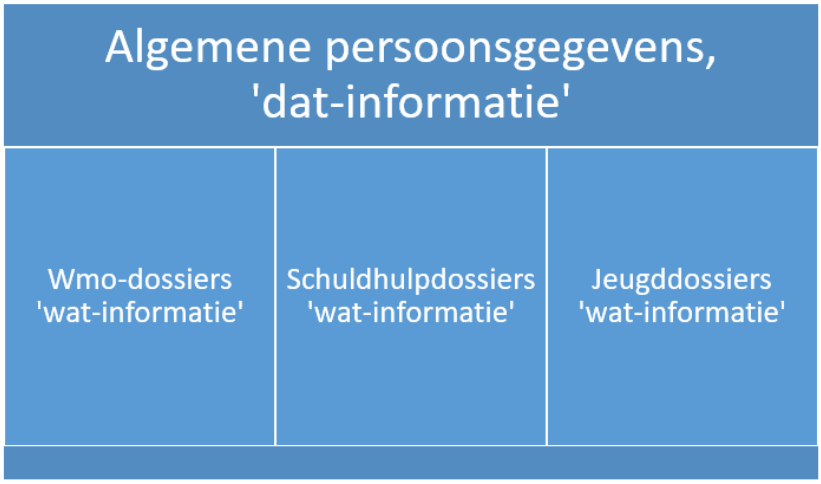

Uitgangspunt zijn de taken die door de medewerkers worden uitgevoerd. Deze taken vloeien voort uit functieomschrijvingen. Om in bestanden verwerkingen uit te kunnen voeren zal men toegang tot die bestanden moeten hebben dmv autorisatie (waar het om digitale bestanden gaat). Het is belangrijk om steeds meerdere mensen te autoriseren voor dergelijke bestanden om te voorkomen dat een situatie ontstaat dat niemand bij de bestanden kan. 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 die 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 bv 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 geautoriseerd worden 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 van de problematiek is en welke verwerking van persoonsgegevens daarbij wenselijk is. Met name bij een multi-probleemsituaties in het sociaal domein kan er opschaling nodig zijn waardoor meer persoonsgegevens worden verwerkt of persoonsgegevens met anderen worden gedeeld. Dit is te rechtvaardigen om te voorkomen dat privacy in de weg gaat staan aan een effectieve hulpverlening. 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 hulpverleningsproces aan het gezin en waarbij meerdere hulpverleners betrokken zijn zullen vanuit deze triage overlegmomenten worden 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 IJsselstein 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 IJsselstein moeten er daarbij rekening mee houden dat het delen met professionele hulpverleners samenhangt met diens geheimhoudingsplichten (en dus niet alles gedeeld kan 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 nog alleen voor de doelen die in de wet staan, dus niet zomaar overal voor.
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 BSN vragen of laten te vermelden in brieven die u naar de gemeente stuurt.

Het is vaak niet nodig dat de gemeente een BSN opneemt in aan burgers gerichte brieven. En dan mag het ook niet. Wel kan de gemeente vragen om een BSN te vermelden bij bepaalde verzoeken of vragen aan de gemeente. Maar dat mag alleen als zo'n verzoek of vraag gaat over een persoonlijke situatie waarbij de medewerker duidelijk wil vaststellen om wie het gaat.
Heeft u een algemene vraag aan de gemeente, bijvoorbeeld over afval? Dan hoeft u uw BSN niet te vermelden.

Om BSN in goede banen te leiden zal er apart onderzoek worden gedaan naar het verwerken van persoonsgegevens met BSN of aan de hand van BSN. De insteek zal zijn 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 reeds is aangegeven ligt de ambtelijke verantwoordelijkheid voor het verwerken van persoonsgegevens bij de afdelingsmanager. Zij brengen in beeld en bewaken het overzicht van de gegevensverwerkingen die op de afdeling plaatsvinden.
Kader van het overzicht wordt gevormd door artikel 30 van de AVG. Zo zal onder meer vastgesteld moeten zijn dat de verwerking een gerechtvaardigd doel kent en gebaseerd is op een rechtmatige grondslag. Uiteindelijke levert dit het volgende plaatje op:

| Verwerkingsregister | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Taakverantwoordelijke | Naam verwerking/proces | Doel verwerking | Betrokkenen | Persoonsgegevens | Bijzondere persoonsgegevens | Ontvangers | Grondslag | Bewaartermijnen | Beschrijving beveiligingsmaatregelen |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |

Het overzicht van gegevensverwerkingen wordt geleverd aan de PO die een register houdt van alle verwerkingen van persoonsgegevens binnen de gemeente IJsselstein. Aan de hand van het register van verwerkingen zal de FG toezicht houden 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 reeds 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 uitgevoerd worden, omdat de meeste processen 'doorontwikkeld' worden en ook later nog privacyrisico's kunnen worden ingedamd.

Het is niet noodzakelijk om voor alle processen waarbij persoonsgegevens worden verwerkt een PIA uit te voeren. Om die reden is er een onderscheid aangebracht en zullen in 2018 enkel PIA's worden 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 zullen de PIA's worden 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 omgegaan moet worden met de belangen van personen die persoonsgegevens aan de gemeente IJsselstein 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 IJsselstein wordt veel aandacht gegeven aan het bewustwordingsproces.

### 8.2 Bewustwording

Momenteel is binnen de gemeente IJsselstein volop aandacht voor het thema privacy. Samen met de CISO en de PO (waar deze zijn aangewezen) 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 zullen de komende tijd PIA's worden uitgevoerd. De PIA zal de eerste periode worden 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 zal ook een bron vormen voor communicatie naar de afdelingen. Na vaststelling van het beleidsplan wordt het plan met de afdelingen besproken. Met de teamleiders zal vervolgens een lijn worden uitgedacht om jaarlijks activiteiten rond het thema 'privacy en informatieveiligheid' te bedenken met daarin aandacht voor bewustwording en gegevensbeveiliging.

### 8.3 Bewustwording door afdelingsactiviteiten

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 IJsselstein (vrijwel) altijd digitaal opgeslagen. Voor opslag van gegevens beschikken de gemeente IJsselstein over een eigen, afgeschermd netwerk. De manier waarop gemeente IJsselstein haar netwerk en gegevens beveiligen 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 persoonsgegeven zijn in de gemeente IJsselstein opgenomen in centrale databases.
- Binnen decentrale databases en spreadsheets die middels algemene kantoorautomatiseringssoftware te benaderen zijn. Dit betreft kleinschalige registraties met een zeer specifiek doel.
- Op ongestructureerde basis: in documenten, afbeeldingen en dergelijke. Dit betreft geen registraties maar specifieke persoonsgegevens over een of enkele personen.

Voor de opslag van persoonsgegevens gelden de volgende uitgangspunten:

- Opslag in centrale databases heeft sterk de voorkeur boven decentrale opslag. Centrale databases kennen een hogere beschikbaarheid, daarnaast is de integriteit en de vertrouwelijkheid van de data veel beter te waarborgen.
- Opslag van persoonsgegevens geschied op goed beveiligde netwerken waarover de gemeente IJsselstein dienen te beschikken.
- Aan medewerkers die geregeld met persoonsgegevens op pad gaan zal een beveiligde voorziening worden aangeboden (smartphone, notebooks).
- Lokale opslag zoals smartphones en laptops worden afdoende versleuteld.

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

De benodigde toegangsrechten worden vastgesteld door het 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. Gemeente IJsselstein kent procedures om deze login te gebruiken bij privacyincidenten.

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

**VERWERKERSOVEREENKOMST UITVOERING <NAAM HOOFDOVEREENKOMST>**

De <naam gemeente>, verder te noemen Verwerkingsverantwoordelijke, hierbij rechtsgeldig vertegenwoordigd door de <heer of mevrouw> <persoonsnaam>, <functie>

en

<Bedrijf>, gevestigd te <plaatsnaam>, verder te noemen Verwerker, hierbij rechtsgeldig vertegenwoordigd door de <de heer of mevrouw>, <persoonsnaam> , <functie>,

hierna afzonderlijk te noemen "Partij", of gezamenlijk "Partijen"

Overwegen het volgende:

a) Partijen op <datum> de <titel hoofdovereenkomst>, hierna Hoofdovereenkomst, hebben afgesloten, op grond waarvan Verwerker de volgende dienst(en) levert aan de Verwerkingsverantwoordelijke: <specificatie dienst(en)>;
b) Verwerker verwerkt voor de uitvoering van de Hoofdovereenkomst Persoonsgegevens voor Verwerkingsverantwoordelijke;
c) Op de verwerking van Persoonsgegevens door Verwerker zijn de Algemene Verordening Gegevensbescherming (AVG) en de Uitvoeringswet AVG van toepassing;
d) Partijen willen in aanvulling op de AVG en de Uitvoeringswet AVG de volgende afspraken over de verwerking van Persoonsgegevens vastleggen in deze Verwerkersovereenkomst;

*Artikel 1 Definities*

1.1 Begrippen uit de AVG en de Uitvoeringswet AVG die in deze Verwerkersovereenkomst worden gebruikt, hebben dezelfde betekenis.
1.2 Bijlagen: aanhangsels bij deze Verwerkersovereenkomst, die deel uitmaken van deze Verwerkersovereenkomst.

*Artikel 2 Ingangsdatum en duur*

2.1 Deze Verwerkersovereenkomst gaat in op het moment van ondertekening en geldt zolang de Hoofdovereenkomst van kracht is, of zolang nog niet is voldaan aan de eisen van artikel 7.1 van deze Verwerkersovereenkomst.

*Artikel 3 Onderwerp van deze Verwerkersovereenkomst*

3.1 Verwerker verwerkt de door of via Verwerkingsverantwoordelijke ter beschikking gestelde Persoonsgegevens uitsluitend in opdracht van Verwerkingsverantwoordelijke voor de uitvoering van de Hoofdovereenkomst behalve als wettelijke verplichtingen of bindende uitspraken van bevoegde organen, anders bepalen.
3.2 De door Verwerker uit te voeren verwerkingen staan in Bijlage 1, die Verwerker met behulp van Verwerkingsverantwoordelijke invult.

*Artikel 4 Verwerker*

4.1 Verwerker moet zorgen voor passende technische en organisatorische maatregelen om de gegevens goed te beveiligen, zoals bedoeld in artikel 32 AVG. Verwerker toont dit aan in Bijlage 2.
4.2 Verwerker mag niets beslissen over de persoonsgegevens die hij heeft ontvangen voor de uitvoering van de Hoofdovereenkomst. Zo neemt hij geen beslissingen over de ontvangst en het gebruik van deze gegevens, de verstrekking aan derden en de duur van de opslag van gegevens.
4.3 Personen die werken voor Verwerker, en Verwerker zelf, moeten de Persoonsgegevens waarmee zij werken geheimhouden, behalve als er een wettelijke uitzondering is. De personen die werken voor Verwerker hebben daarom een geheimhoudingsverklaring getekend. De geheimhouding geldt ook nog na afloop van deze Verwerkersovereenkomst.
4.4 Verwerker mag - met toestemming van Verwerkeringsverantwoordelijke - voor de uitvoering van de werkzaamheden een andere verwerker inschakelen. Verwerker laat voor de ingangsdatum aan Verwerkingsverantwoordelijke weten wie de andere ingeschakelde verwerkers zijn. Verwerker vult daarvoor tabel 3 van Bijlage 1 in en houdt deze actueel.
4.5 Als Betrokkene een beroep doet op zijn rechten (o.a. inzage, correctie, verwijdering), helpt Verwerker Verantwoordelijke om daarop binnen de wettelijke termijnen een beslissing te nemen.
4.6 Als Verwerkingsverantwoordelijke een gegevensbeschermingseffectbeoordeling, of een audit wil uitvoeren en de hulp van Verwerker daarbij nodig heeft, dan maken Partijen daarover afspraken.

*Artikel 5 Inbreuk in verband met Persoonsgegevens*

5.1 Verwerker zal Verwerkingsverantwoordelijke zo snel mogelijk, maar uiterlijk 48 uur na ontdekking van een inbreuk in verband met Persoonsgegevens, hierover informeren. Daarbij verstrekt Verwerker zonder onredelijke vertraging alle noodzakelijke informatie, medewerking en toegang aan Verwerkingsverantwoordelijke, zodat laatstgenoemde de Inbreuk op tijd kan melden aan de Autoriteit Persoonsgegevens en/of Betrokkene overeenkomstig de AVG.
5.2 In geval van een Inbreuk neemt Verwerker zo snel mogelijk alle maatregelen om de Inbreuk te herstellen, de gevolgen van de Inbreuk te beperken en verdere Inbreuken te voorkomen.
5.3 Verwerker heeft een gedegen plan van aanpak over de omgang met en de afhandeling van Inbreuken en zal Verwerkingsverantwoordelijke, op zijn verzoek, dat plan laten zien.
5.4 Verwerker heeft een gedetailleerd logboek van alle Inbreuken en de maatregelen die op Inbreuken zijn genomen. Verwerkingsverantwoordelijke mag dat inzien, wanneer deze daarom vraagt.
5.5 Verwerkingsverantwoordelijke beslist of deze de Inbreuk moet melden bij de toezichthoudende autoriteit en/of Betrokkene.

*Artikel 6 Aansprakelijkheid*
6.1 De Partij die toerekenbaar tekortschiet in de nakoming van zijn verplichtingen, is tegenover de andere Partij aansprakelijk voor de door deze geleden en/of te lijden schade.
6.2 De aansprakelijkheid voor schade, uit welke hoofde dan ook, is beperkt tot viermaal de hoogte van de vergoeding per gebeurtenis, waarbij de aansprakelijkheid nooit meer bedraagt dan € 5.000.000,-.

*Artikel 7 Beëindigen verwerkersovereenkomst*
7.1 Na afloop van de werkzaamheden, zal Verwerker op verzoek van Verwerkingsverantwoordelijke de ter beschikking gestelde Persoonsgegevens aan Verwerkingsverantwoordelijke teruggeven en/of vernietigen.
7.2 Verwerkingsverantwoordelijke kan nadere redelijke eisen stellen aan de wijze van beschikbaarstelling, waaronder eisen aan het bestandsformaat, dan wel vernietiging. Deze werkzaamheden moeten, binnen een nader overeen te komen redelijke termijn, uitgevoerd worden.
7.3 Verwerker maakt hiervan een verslag en geeft dit aan Verwerkingsverantwoordelijke.

*Artikel 8 Overige bepalingen*
8.1 Alle geschillen, ook als alleen één Partij vindt dat er een geschil is, zullen in eerste instantie worden voorgelegd aan de bevoegde rechter van de Rechtbank < vul in>.
8.2 Alle rechten en verplichtingen uit de Hoofdovereenkomst, waaronder begrepen de van toepassing zijnde algemene voorwaarden, zijn voor het overige aanvullend van toepassing op de verwerking van Persoonsgegevens.

**Ondertekening**

Aldus overeengekomen en in tweevoud ondertekend,

*Gemeente* **<naam gemeente>**
Namens: < naam, functie

plaats: <……..>

datum: <……..>

<**Naam organisatie**>
namens deze< naam, functie deze>

plaats: <……..>

datum: <……..>

**BIJLAGE 1**

**Overzicht van te verwerken persoonsgegevens**

1. *Naam verwerking, doeleinden, categorieën van betrokkenen, (bijzondere) persoonsgegevens en eventuele doorgifte naar derde landen*

| Naam verwerking | Verwerkingsdoeleinden | Categorieën van Betrokkenen | (Bijzondere) Persoonsgegevens | Doorgifte naar derde landen |
|---|---|---|---|---|
| | | | | |

| | | | | |
|---|---|---|---|---|
| | | | | |
| | | | | |

2. *Contactgegevens*

| | |
|---|---|
| **Contactpersoon Verwerkingsverantwoordelijke (NB: Ook buiten kantoor-uren)** | Naam:<br>Contactgegevens: |
| **Contactpersoon Verwerker (NB: Ook buitenkantooruren)** | Naam:<br>Contactgegevens: |
| **Contactgegevens IBD** | Telefoonnummer 070-373 8011 |

3. *Ingeschakelde subverwerkers*

| **Naam en contactgegevens subverwerker** | **Uitbestede verwerkingen** |
|---|---|
| | |
| | |
| | |
| | |

NB: Eventuele wijzigingen in bovenstaande tabellen geven partijen op korte termijn aan elkaar door.

**BIJLAGE 2**

*Aantonen passend niveau van beveiliging*

1. Normenstelsel
   - ☐ De informatiebeveiliging vindt plaats volgens algemeen erkende normen, namelijk:

     ……
     ……..(vermeld normenstelsel, zoals bijvoorbeeld NEN7510, NEN/ISO 27001, PCI/DSS).
   - ☐ De informatiebeveiliging vindt plaats volgens een algemeen erkende overheidsnorm zoals de BIG (of de BIR, BIO) of vergelijkbaar, namelijk:

     ……..

2. De toereikendheid van de informatiebeveiliging blijkt uit:
   - ☐ Periodieke externe controles zoals audits of TPM's (bijv. ISAE3xxx SOC type II);
   - ☐ Een Assurance rapport van een auditor die is aangesloten bij NOREA;
   - ☐ Data Pro Certificaat
   - ☐ Eigen controles of eigen mededelingen over de beveiligingsmaatregelen zoals hieronder beschreven:
   - ☐ ……

Uit de certificering/periodieke externe controles/audits of uit de eigen controles/beschrijvingen blijkt of kan afgeleid worden dat de beveiliging passend is bij de verwerking(en) genoemd in bijlage 1.

## 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.

## 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 ondergetekenden:

Het college van burgemeester en wethouders van de gemeente:

en,

Naam: ……..

Komen als volgt overeen:

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 opgemaakt in tweevoud op …….. te ….

Afdelingsmanager

……..

U

……..

## Bijlage 4 Activiteitenoverzicht en kostenraming implementatie

Na vaststelling van het beleidsplan privacy zullen een aantal activiteiten worden 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.

| Activiteit | Verantwoordelijkheid | Concl. A3P | Uren | Incidenteel Structureel | Planning |
|---|---|---|---|---|---|
| Toedeling thema privacy aan portefeuillehouder | College | | 2 | I | |
| Mandaatbesluit ondertekening verwerkersovereenkomst en protocollen | College en jurist Awb | | 8 | I | |
| Inrichting van het privacy-platform (driehoek), inclusief centraal communicatiemiddel, en aanstellen van medewerkers (zie H5) | Manager bedrijfsvoering | 13 | 12 | S | |
| Inrichten en bijhouden van het register van verwerkingen en het overzicht verwerkersrelaties | Privacy officer | 2 | 80 | S | |
| Passende technische maatregelen voor veilig gebruik persoonsgegevens conform artikel 25 AVG | | | 200 | S | |
| Inhaalslag tzv ontbrekende contracten of protocollen en het bijhouden van deze registers | Privacy officer | 4,13 | 200 | S | |
| Werkinstructies opstellen voor:<br>- Uitvoeren rechten van betrokkenen (Art 15 ev. AVG)<br>- Behandelen bezwaren van betrokkenen (Art 21 AVG) | Privacy officer | 12,20 | 16 | I | |
| Werkinstructies opstellen voor:<br>- Veilig delen van persoonsgegevens (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 | Teamleiders | 3, 6, 8, 9, 10, 12, 14, 15, 16, 17, 18, 19, 20 | 60 | I | |
| Vaststellen takenpakket medewerkers en toegang tot bestanden | Teamleiders | 5, 7 | 120 | S | |
| Aanschaf beveiligde devices voor gebruik buitenshuis, inrichten en instrueren | Teamleiders die het aangaat | | 20 | I | |
| Integratie van privacy- en veiligheidsbeleid in de jaarlijkse planning en controlcyclus | Controller | 1 | 8 | I | |
| Opstellen jaarlijks activiteitenplan bewust omgaan met persoonsgegevens | Teamleiders | 13 | 12 | S | |
| Opstellen communicatieschema bewust omgaan met persoonsgegevens (intern en extern) | Communicatiemanager | 11 | 160 | S | |
| Inrichten risk-based toezichtsmodel (mede aan de hand van PIA's)<br>Uitvoeren PIA's en trainen medewerkers | Functionaris gegevensbescherming | | 120 | I | |
| Projectleider implementatie bovengenoemde activiteiten | Projectleider AVG | | 120 | 1 | |

## Bijlage 5 protocol datalekken

**Procedure meldplicht datalekken  Gemeente IJsselstein**

**1. INLEIDING**

**1.1 Aanleiding**

Vanaf 1 januari 2016 is de meldplicht Datalekken van kracht. Dit houdt in dat de gemeente verplicht is om (potentiële) datalekken te melden aan de toezichthouder, de Autoriteit Persoonsgegevens, en in bepaalde gevallen ook aan de betrokkene van wie de gegevens zijn gelekt. Als blijkt dat niet of onvoldoende is voldaan aan deze meldplicht kan de toezichthouder een boete opleggen tot € 20 miljoen of 4% van de jaarlijkse wereldwijde omzet per overtreding.

Een datalek dient uiterlijk *binnen 72 uur* na ontdekking van het datalek te worden gemeld aan de toezichthouder. Indien dit later gebeurt, dan dient de melding voorzien te worden van uitleg omtrent de vertraging.

Niet ieder datalek-incident valt onder de meldplicht. Er is sprake van een zogeheten geclausuleerde meldplicht voor datalekken. Hiervoor is het noodzakelijk dat een juridische beoordeling wordt gemaakt. Artikel 33(1) van de AVG stelt dat een datalek alleen gemeld dient te worden wanneer er een aanzienlijk risico is op schade aan de persoonlijke levenssfeer van een individu. Als bijvoorbeeld verloren of gesloten persoonsgegevens goed versleuteld zijn opgeslagen, dan is er geen aanzienlijke risico op schade aan de persoonlijke levenssfeer.

**1.2 Doel en reikwijdte**

Deze procedure beschrijft de wijze waarop binnen de gemeentelijke organisatie wordt omgegaan met de meldplicht datalekken in de zin van de Algemene Verordening Gegevensbescherming (AVG). Het bevat afwegingskaders bij een vermoeden van een datalek en specificeert de nodige acties.

Binnen de gemeente IJsselstein worden de volgende stappen in de procedure gehanteerd:
1) het signaleren, analyseren en registreren van incidenten waarbij er sprake is van een inbreuk op een beveiligingsmaatregel en persoonsgegevens bij betrokken zijn;
2) het inhoudelijk beoordelen en onderzoeken van het incident of er op grond van de AVG sprake is van een datalek dat gemeld moet worden;
3) het melden van het datalek aan de toezichthouder en betrokkenen namens het bestuur;
4) het nemen van maatregelen om het lek te dichten;
5) het documenteren van het datalek bij zowel interne als externe meldingen.

Hieronder volgt een nadere uitwerking van deze procedure.

**2. PROCEDURE DATALEK**

**2.1  Melden incident bij Chief Information Security Officer (CISO)**

De meldplicht datalekken geldt voor de gehele organisatie en iedere medewerker. Iedere medewerker die te maken heeft met vermissing/diefstal van zaken die van de gemeente zijn, of met een informatiebeveiligingsincident, dient dit te melden bij de CISO. Dit kan telefonisch via toestelnummer ---------- of via het emailadres privacy@ijsselstein.nl

De medewerker wordt verzocht zijn/haar naam en contactgegevens in het formulier in te vullen met de informatie over het incident. De melder kan namelijk gevraagd worden om aanvullende informatie te geven over het incident. Dit is belangrijk voor de goede en snelle afhandeling van het incident en de volledigheid voor een eventuele melding aan de Autoriteit Persoonsgegevens.

Indien de medewerker twijfelt of er sprake is van een incident of wat hij moet doen, kan hij de privacy adviseur of CISO raadplegen.

**2.1.1 Registratie van het incident**
Zodra melding is gedaan bij de CISO, meldt hij het incident bij de supportmedewerker en registreert hij de incidentmelding in datalekregister.
De CISO analyseert of er bij het incident persoonsgegevens betrokken zijn. Indien de melding telefonisch is gedaan, vraagt de CISO dit na bij de melder.

Indien bij het datalek persoonsgegevens betrokken zijn, zorgt de supportmedewerker dat de melding wordt doorgestuurd naar de privacy adviseur.

**2.2 Vaststelling datalek**

**2.2.1.Taak CISO en privacy officer**

De CISO en privacy officer beoordelen samen of er een aanzienlijk risico is op schade aan de persoonlijke levenssfeer van een individu. Bij afwezigheid van de CISO en/of de privacy adviseur beoordeelt de Functionaris Gegevensbescherming (FG) het risico.

Indien wordt geconstateerd dat er sprake is van een meldenswaardig datalek, dan zorgt de privacy officer ervoor dat de FG zo snel mogelijk (telefonisch) wordt geïnformeerd. De privacy officer stuurt aanvullend een e-mail met een gemotiveerde beoordeling en een advies van het incident. Indien de privacy officer en CISO beoordelen dat het incident geen datalek in de zin van de AVG betreft, dan zorgt de privacy officer ervoor dat de beoordeling schriftelijk wordt teruggekoppeld aan de melder. Een afschrift van het advies wordt aan de FG toegezonden en aan de supportmedewerker. De supportmedewerker vult de oorspronkelijke melding in de registratie aan met de beoordeling van het incident.

De privacy officer is er verantwoordelijk voor dat het meldingsformulier van de toezichthouder wordt ingevuld en vervolgens wordt toegestuurd naar de toezichthouder. Vanwege het gegeven dat verwerkingsverantwoordelijke binnen 72 uur behoort te melden aan de toezichthouder dient de melding door alle betrokken medewerkers direct en met hoogste prioriteit te worden opgepakt.

**2.2.2. Taak van de Functionaris Gegevensbescherming**
Is sprake van een datalek dan zal de FG worden geïnformeerd. Hij zal op de hoogte gehouden worden van alle stappen die in het proces worden gedaan en toezicht houden op een correcte afhandeling. In de verantwoordingscyclus zal verslag worden gedaan van het aantal en soort datalekken en de wijze waarop de organisatie het datalek heeft aangepakt

**2.2.3 Beslisboom voor de melding aan toezichthouder**

Er is sprake van een geclausuleerde meldplicht voor datalekken. Dat wil zeggen dat alleen een inbreuk hoeft te worden gemeld als deze leidt tot een aanzienlijk risico op schade aan de persoonlijke levenssfeer van betrokkenen. Hierbij spelen de volgende factoren een rol:

1) Zijn er persoonsgegevens van gevoelige aard gelekt? Het betreft hier een incident waarbij bijzondere persoonsgegevens zoals medische/politiegegevens gegevens over ras of religie of financiële gegevens zijn gelekt.
2) Leiden de aard en omvang van de inbreuk tot een aanzienlijk risico op schade aan de persoonlijke levenssfeer van een individu? Naarmate er meer gevoelige gegevens in het geding zijn (ofwel van meerdere personen ofwel veel gegevens van een persoon) zal er eerder sprake zijn van een datalek dat moet worden gemeld.

Er moet in ieder geval gemeld worden als één van onderstaande vragen positief wordt beantwoord.

| |
|---|
| Zijn gegevens (definitief) verloren gegaan?<br><br>Ja ➔ melden |
| Zijn de gegevens bijzonder of zeer omvangrijk?<br><br>Ja ➔ melden |
| Zijn de gegevens in onbevoegde handen geraakt?<br><br>Ja ➔ melden |
| Aanzienlijk risico op schade aan persoonlijke levenssfeer?<br><br>Ja ➔ melden<br><br>Nee op alle vragen àniet melden |

Mogelijk is op het moment dat er gemeld moet worden nog geen volledig zicht op wat er gebeurd is en om welke persoonsgegevens het gaat. In dat geval vindt de melding plaats op basis van de gegevens

waarover de gemeente op dat moment beschikt. Eventueel kan de melding naderhand nog worden aangevuld of zelfs worden introkken.

**2.2.4. Melden aan betrokkene?**

De betrokkene is degene over wie persoonsgegevens worden verwerkt en waarvan de gegevens onderwerp zijn van de datalek. Indien er sprake is van een datalek moet deze aan de betrokkene worden gemeld, als de inbreuk een hoog risico brengt op schade aan diens persoonlijke levenssfeer. Niet in alle gevallen hoeft een datalek aan de betrokkene te worden gemeld.

Voor de beoordeling of aan de betrokkene(n) gemeld moet worden, zijn de volgende vragen van belang.

| |
|---|
| Zijn er zwaarwegende redenen om de melding aan de betrokkene achterwege te laten? |
| |
| Nee ➔ Melden burger |

| |
|---|
| Zijn de gegevens versleuteld of ontoegankelijk voor degene die geen recht op inzage heeft in deze gegevens? |
| |
| Nee ➔ Melden burger |

Artikel 34, lid 3 AVG stelt drie voorwaarden waaronder geen melding aan betrokkenen vereist is.
Dit geldt in de volgende situaties:

1. Er zijn technische en organisatorische maatregelen getroffen ter bescherming van de persoonsgegevens vooraf aan het lek. In het bijzonder maatregelen die ervoor zorgen dat de data niet toegankelijk is voor ongeautoriseerde personen. Bijvoorbeeld door encryptie of anonimiseren.
2. Direct na een datalek zijn er acties ondernomen om ervoor te zorgen dat er geen hoog risico meer is op schade aan de persoonlijke levenssfeer van betrokkenen.
3. Het zou van onevenredige moeite zijn om contact op te nemen met individuen, bijvoorbeeld wanneer de contactgegevens van betrokkenen verloren zijn. In dit geval zal er gekozen moeten worden voor een openbare communicatie uiting of een vergelijkbare maatregel.

**2.2.5. Melden aan het college van burgemeester en wethouders**

Het college van burgemeester en wethouders is eindverantwoordelijk voor het voldoen aan de meldplicht datalekken. Op grond van de mandaatregeling meldt de privacy adviseur namens het college het datalek aan de toezichthouder en zorgt voor de verdere vervolgacties die kunnen voortkomen uit de melding.

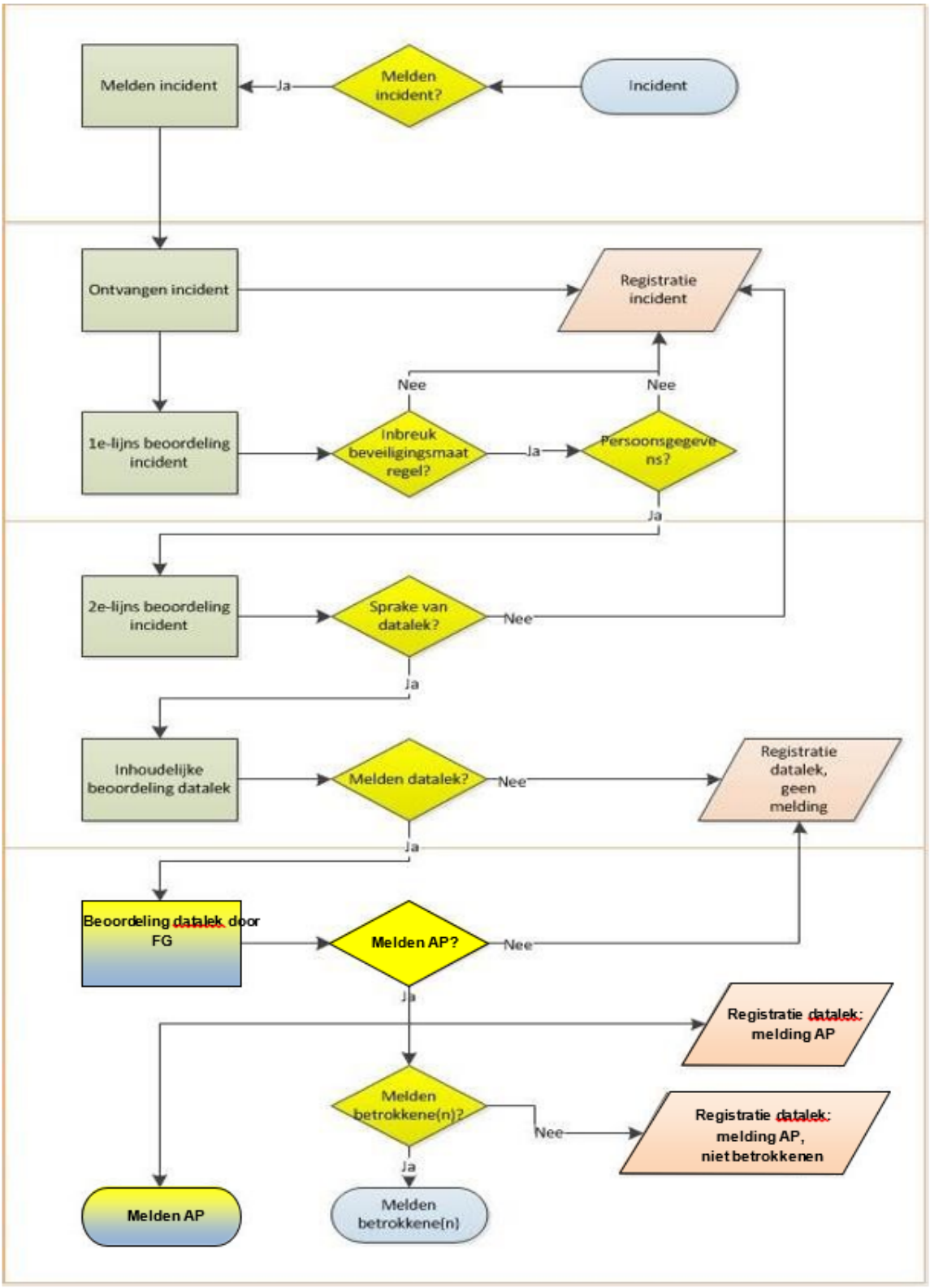
Het is van belang dat bij een datalek de verantwoordelijke bestuurders geïnformeerd worden. De noodzaak hiervan neemt toe, naarmate er sprake is van een incident waarbij veel partijen betrokken zijn en veel gevoelige informatie verloren is gegaan. Ook kan het noodzakelijk zijn de bestuurders te informeren indien het incident betrekking heeft op de gemeente als geheel of er veel aandacht is in de media/pers voor een incident. Het afdelingshoofd van de dienst waar het datalek is ontstaan informeert de burgemeester of de wethouder die verantwoordelijk is voor privacy.

**2.2.6. Melden aan andere partijen?**

Indien sprake is van samenwerking met andere partijen (ketenverwerking of verwerkers) zal de gemeente moeten beoordelen of een datalek-incident aan de externe partij gemeld moet worden.
Dit is geen wettelijke verplichting, maar kan vanuit communicatie redenen raadzaam zijn.
Bij de uitwerking van de communicatiestrategie vindt afstemming plaats welke doelgroepen/ overige partijen worden geïnformeerd over het datalek en op welke wijze.

**3. AFHANDELEN MELDING**
Nadat de Privacy adviseur heeft vastgesteld dat het een datalek in de zin van de AVG betreft en waarbij melding is gedaan bij de Autoriteit Persoonsgegevens, dan zorgt de privacy adviseur ervoor dat de beoordeling schriftelijk wordt teruggekoppeld aan de melder en de supportmedewerker. De supportmedewerker vult de oorspronkelijke melding in de registratie aan met de beoordeling van het datalek en de bevindingen van de FG, het college en de Autoriteit Persoonsgegevens.

**Stroomschema datalekken**


Melden incident
Ja
Melden incident?
Incident
Ontvangen incident
Registratie incident
Nee
Nee
1e-lijns beoordeling incident
Inbreuk beveiligingsmaat regel?
Ja
Persoonsgegevens?
Ja
2e-lijns beoordeling incident
Sprake van datalek?
Nee
Ja
Inhoudelijke beoordeling datalek
Melden datalek?
Nee
Registratie datalek, geen melding
Ja
Beoordeling datalek door FG
Melden AP?
Nee
Ja
Registratie datalek: melding AP
Melden betrokkene(n)?
Nee
Registratie datalek: melding AP, niet betrokkenen
Ja
Melden AP
Melden betrokkene(n)