LISSE

GEMEENTEBLAD

Officiële uitgave van de gemeente Lisse

Nr. 195458

5 augustus 2019

Privacybeleid gemeente Lisse

1. Aanleiding

Vanaf 25 mei 2018 is de Algemene Verordening Gegevensbescherming (hierna: AVG) van toepassing. Deze verordening is de opvolger van de - nationale - Wet bescherming persoonsgegevens (Wbp). De AVG zorgt samen met de Uitvoeringswet AVG onder andere voor versterking en uitbreiding van de privacyrechten voor betrokkenen met meer verantwoordelijkheden voor organisaties die persoonsgegevens verwerken.

2. Waarom dit beleid?

De gemeenten Hillegom, Teylingen en Lisse werken samen in de werkorganisatie HLTsamen (hierna: HLTsamen). Binnen de verschillende domeinen van dit samenwerkingsverband worden veel, bijzondere en gevoelige persoonsgegevens verwerkt. Daarom zijn de afzonderlijke gemeenten en HLTsamen verplicht om een gegevensbeschermingsbeleid te hebben ter voorkoming van misbruik. Door het hanteren van het gegevensbeschermingsbeleid (hierna: 'privacybeleid') kunnen de afzonderlijke gemeenten en HLTsamen ook aantonen dat aan de verantwoordingsplicht uit de AVG wordt voldaan. Verder kan dit privacybeleid eraan bijdragen dat besluiten op grond van de AVG binnen de afzonderlijke gemeenten en HLTsamen op een eenduidige manier worden genomen en dat ook de procedures eenduidig zijn voor iedereen die te maken krijgt met verwerking van persoonsgegevens.

Maar belangrijker, de afzonderlijke gemeenten en HLTsamen wil transparantie naar de inwoners toe betrachten en deze informeren. De burger moet erop kunnen vertrouwen dat HLTsamen zorgvuldig en veilig met de persoonsgegevens omgaat.

De AVG verplicht de gemeenten en HLTsamen om steeds te kijken of het beleid nog voldoet en of het aangepast moet worden. Technologische en maatschappelijke ontwikkelingen volgen elkaar snel op. Dit kan reden zijn om het beleid periodiek aan te passen. Er is immers sprake van nieuwe wetgeving, die volop in beweging is, en waar door de rechtspraak en de toezichthouder nog nader invulling aan wordt gegeven.

Reikwijdte

Dit beleid is van toepassing op de gehele organisatie, alle processen, onderdelen, objecten en gegevensverzamelingen van HLTsamen en de (bestuursorganen) van de in deze gemeenschappelijke regeling deelnemende gemeenten, uitgezonderd de gemeenteraad en de heffingsambtenaar.

Vaststelling

Het privacybeleid wordt door de afzonderlijke colleges van de drie gemeenten en het bestuur van de werkorganisatie HLTsamen vastgesteld.

Uitwerking

De kaders uit het privacybeleid vormen het uitgangspunt voor nader uit te werken beleidsregels, gedragsrichtlijnen en protocollen of om deze te actualiseren. Deze beleidsregels, gedragsrichtlijnen en protocollen geven richting aan de uitvoering in de dagelijkse praktijk. Het gaat in ieder geval om de volgende (niet limitatief):

- Privacyprotocol dat richtlijnen en handvatten voor alle medewerkers bevat,
- Reglementen / procedures per werkproces waarin frequent en systematisch persoonsgegevens verwerkt worden,
- Email-protocol,
- Privacyreglement Sociaalteams,
- Procedures en richtlijnen AVG BRP,
- Protocol: informatiebeveiligingsincidenten en datalekken HLTsamen,
- Protocol gebruik thuiswerkplek .

Naast deze documenten/handreikingen kunnen in de toekomst nog meer richtlijnen, protocollen en beleidsregels worden opgesteld. Hiermee kunnen we snel en flexibel inspelen op nieuwe ontwikkelingen.

3. Wettelijke kaders

De verwerkingen van persoonsgegevens zijn gebonden aan eisen uit wet- en regelgeving.
De belangrijkste wettelijke kaders met betrekking tot privacybescherming zijn:

1. Artikel 8 Europees Verdrag voor de Rechten van de Mens
2. Artikelen 10 t/m 13 Grondwet
3. Algemene Verordening Gegevensbescherming (en de Uitvoeringswet AVG)

4. Sectorale wetgeving zoals:
   - Wet maatschappelijke ondersteuning 2015 (Wmo)
   - Jeugdwet
   - Participatiewet
   - Drank- en Horecawet
   - Wet algemene bepalingen omgevingswet (Wabo);
   - Wet milieubeheer
   - Wet openbaarheid van bestuur

5. Archiefwet
6. Het Wetboek van Strafrecht

Interne kaders
* Integriteitsbeleid
* Informatiebeveiligingsbeleid

4. Samenhang Privacybeleid met Informatiebeveiligingsbeleid

Bescherming van persoonsgegevens en informatiebeveiliging zijn nauw met elkaar verbonden. In het volgende plaatje wordt een en ander verduidelijkt.

5. Visie en uitgangspunten

Visie

Onze inwoners kunnen erop vertrouwen dat wij hun privacy respecteren en zorgvuldig omgaan met hun persoonsgegevens. De bescherming van persoonsgegevens passen wij toe in onze dienstverlening en in de beleidskeuzes die wij maken conform het privacybeleid. Technologische- en maatschappelijke ontwikkelingen dwingen ons ertoe dat wij het privacybeleid voortdurend aanpassen. In onze afwegingen zijn wetgeving en de 'menselijke maat' voor het beschermen van de privacy van de inwoners belangrijke kaders. Privacybescherming is een onderwerp dat voor bestuurders en medewerkers een integraal onderdeel van het werk vormt.

Uitgangspunten

HLTsamen en de afzonderlijke gemeenten binnen dit samenwerkingsverband gaan op een veilige manier met persoonsgegevens om en respecteren de privacy van betrokkenen (inwoners en medewerkers). Zij houden zich hierbij aan de volgende uitgangspunten:

A. Rechtmatigheid, behoorlijkheid, transparantie

Persoonsgegevens worden in overeenstemming met de wet- en regelgeving en op behoorlijke, zorgvuldige en aantoonbare wijze verwerkt.
Het is van belang dat inwoners vertrouwen hebben in de zorgvuldige verwerking van hun persoonsgegevens. Inwoners krijgen inzicht in en worden helder geïnformeerd over hun rechten en de wijze waarop hun persoonsgegevens worden verwerkt en beheerd. Voor hen moet in elk geval duidelijk zijn:

- Welke persoonsgegevens de gemeente verzamelt (wat)
- Met welk doel (waarom)
- Wat de wettelijke grondslag is (zie verwerkingsgrondslagen)
- Wie toegang heeft tot deze gegevens (wie)
- Wat de gemeente vervolgens verder doet met deze gegevens (wat gebeurt er)
- Hoe lang de gegevens bewaard worden (bewaartermijnen)
- Beveiliging van gegevens.

Transparantie gaat niet in alle gevallen op. Er kan sprake zijn van legitieme uitzonderingen, bijvoorbeeld in situaties die te maken hebben met openbare orde en veiligheid. In dergelijke gevallen kan de gemeente, met inachtneming van wet- en regelgeving, een voorbehoud maken op het transparantiebeginsel.

Bij transparantie hoort ook een open cultuur. De open cultuur helpt de gemeente bij het verder op orde krijgen van het privacybeleid en –beheer. Wij moedigen medewerkers aan incidenten te melden, hiervoor is een laagdrempelige procedure ingericht. Ook inwoners kunnen situaties makkelijk en snel melden, via de reguliere klachtenprocedure en waar nodig ook via een aparte klachten- /meldingsprocedure. De afzonderlijke Colleges van B&W van de drie gemeenten en het bestuur van de werkorganisatie HLTsamen leggen aan de gemeenteraden en aan het maatschappelijk verkeer verantwoording af over de uitvoering van het privacybeleid, inclusief de opgetreden incidenten en klachten.

B. Grondslag en doelbinding
HLTsamen en de afzonderlijke gemeenten zorgen ervoor dat persoonsgegevens alleen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doelen worden verzameld en verwerkt. Persoonsgegevens worden alleen op basis van een rechtmatige grondslag verwerkt. In bijlage 1 is een stroomschema voor het rechtmatig verwerken van persoonsgegevens weergeven.

Verwerkingsgrondslagen
Artikel 6 AVG geeft de grondslagen voor verwerking. Persoonsgegevens mogen alleen worden verwerkt indien één van die grondslagen van toepassing is. Hieronder worden de belangrijkste grondslagen besproken.

Toestemming
Betrokkene heeft toestemming gegeven voor het verwerken van persoonsgegevens voor een of meer specifieke doeleinden.

De AVG verstaat onder toestemming '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.'
In deze definitie zit een aantal elementen:
Van belang is dat de toestemming in vrijheid is gegeven. Als er een afhankelijke relatie bestaat tussen degene die toestemming geeft en degene die de persoonsgegevens wil gebruiken, is de kans groot dat de gegeven toestemming niet in vrijheid is gegeven. Denk aan relatie werkgever-werknemer of in het sociaal domein. In deze situaties kan toestemming veelal niet vrijelijk worden gegeven, gezien de vaak afhankelijke relatie tussen de gemeente en de betrokkene.
Verder dient de toestemming specifiek geïnformeerd te zijn. Dat wil zeggen: deze mag niet te ruim en algemeen geformuleerd zijn en het moet voor de betrokkene duidelijk zijn welke persoonsgegevens voor welke doeleinden verwerkt worden. Toestemming is ondubbelzinnig wanneer er geen onduidelijkheid kan bestaan of de betrokkene daadwerkelijk toestemming heeft gegeven.

Wettelijke verplichting
Het verwerken van persoonsgegevens is noodzakelijk om aan een wettelijke verplichting te voldoen. Een voorbeeld: de Participatiewet verplicht het College van B&W van de afzonderlijke gemeenten in bepaalde gevallen om (persoons)gegevens te verstrekken aan instanties als de Belastingdienst. Om aan deze verplichting te voldoen, is het noodzakelijk dat het college gegevens verwerkt.

Publiekrechtelijke taak
De verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag. Hiervan is bijvoorbeeld sprake als de gemeente een bij wet geregelde - publiekrechtelijke - taak uitvoert. Er moet sprake zijn van een typische overheidstaak. Een voorbeeld hiervan is het beslissen op een aanvraag voor een maatwerkvoorziening op grond van de Wmo 2015.

C. Dataminimalisatie
HLTsamen en de afzonderlijke gemeenten verwerken alleen de persoonsgegevens die noodzakelijk zijn voor het vooraf bepaalde doel. HLTsamen en de afzonderlijke gemeenten streven naar minimale gegevensverwerking: waar mogelijk worden daarbij minder of geen persoonsgegevens verwerkt.

D. Bewaartermijn
Persoonsgegevens worden niet langer bewaard dan nodig is. Het bewaren van persoonsgegevens kan nodig zijn om de gemeentelijke taken goed uit te kunnen oefenen of om wettelijke verplichtingen te kunnen naleven. Voor de bewaartermijnen wordt aangesloten bij de "Selectielijst gemeenten en intergemeentelijke organen 2017".

E. Integriteit en vertrouwelijkheid
HLTsamen en de afzonderlijke gemeenten gaan zorgvuldig om met persoonsgegevens en behandelen deze vertrouwelijk. Zo worden persoonsgegevens alleen verwerkt voor het doel waarvoor deze gegevens zijn verzameld. Daarbij zorgen HLTsamen en de afzonderlijke gemeenten voor passende beveiliging van persoonsgegevens conform het daartoe vastgestelde informatiebeveiligingsbeleid.

F. Delen met derden
In het geval van samenwerking met externe partijen, waarbij sprake is van gegevensverwerking van persoonsgegevens, maakt de gemeente afspraken over de eisen waar gegevensuitwisseling aan moet voldoen. Deze afspraken voldoen aan de wet- en regelgeving. De gemeente controleert deze afspraken periodiek.

G. Subsidiariteit
De inbreuk op de persoonlijke levenssfeer van betrokkenen wordt zoveel mogelijk beperkt. Er wordt altijd bekeken of het doel ook met minder ingrijpende middelen bereikt kan worden.

H. Proportionaliteit
De inbreuk op de belangen van de betrokkene mag niet onevenredig zijn in verhouding tot het met de verwerking te dienen doel.

I. Rechten van betrokkenen
HLTsamen en de afzonderlijke gemeenten honoreren de rechten van betrokkenen behoudens wanneer andere wet- en regelgeving dit belemmert. Het betreft de volgende rechten: verzoek om inzage/afschrift, correctie, verwijdering en/of bezwaar. Voor het uitoefenen van deze rechten wordt een procedure opgesteld en een werkproces ingericht om gestructureerd te kunnen behandelen. In bijlage 2 zijn de procedures algemeen beschreven. Iedere betrokkene heeft het recht op informatie over de persoonsgegevens die de gemeente van hem of haar verwerkt en over het doel waarmee de gegevens worden verwerkt, om deze in te zien en ook om deze gegevens te verbeteren, aan te vullen, te verwijderen of af te schermen als deze feitelijk onjuist, onvolledig of niet ter zake dienend zijn. De afzonderlijke Colleges van B&W van de drie gemeenten en het bestuur van de HLTsamen communiceren actief over deze rechten, op de gemeentelijke websites en in andere uitingen en dragen zorg voor een eenvoudige en toegankelijke wijze waarop inwoners hun rechten kunnen uitoefenen.

J. Verwerkerscontracten
De gemeente of HLTsamen maakt alleen gebruik van verwerkers van persoonsgegevens die voldoende garanties bieden met betrekking tot het toepassen van technische en organisatorische maatregelen om de verwerking te laten voldoen aan de AVG-vereisten. Hiervoor wordt zoveel mogelijk gebruik gemaakt van de model verwerkersovereenkomst van de Informatiebeveiligingsdienst (IBD).

K. Selectie op basis van gegevensbescherming door ontwerp en door standaardinstellingen
Om de zes beginselen van privacybescherming, zoals hiervoor verwoord bij verwerkingsgrondslagen onder B, zo goed mogelijk door te voeren, nemen HLTsamen en de afzonderlijke gemeenten juist ook aan de voorkant van het ontwerpen en inrichten van processen en systemen privacybescherming als uitgangspunt. Hiertoe worden de volgende instrumenten te worden ingezet: privacy by design, privacy by default en het vooraf uitvoeren van een Data protection impact assessment (DPIA).

Privacy by design
Privacy by design houdt in dat er al bij het ontwerpen van producten en diensten voor gezorgd wordt dat persoonsgegevens goed worden beschermd.
Bij de inrichting van een proces of systeem wordt gekeken naar de eisen die vanuit de invalshoek van privacy gesteld kunnen worden. Dataminimalisatie is bijvoorbeeld één van de uitgangspunten die hierbij gehanteerd worden: zo min mogelijk persoonsgegevens verzamelen, alleen datgene wat strikt noodzakelijk is voor het bereiken van het doel. Ook kunnen privacy-verhogende maatregelen worden meegenomen, bijvoorbeeld door gevoelige gegevens in een afgesloten bestand te bewaren.
Voorbeelden van privacy by design:

- het op eenvoudige wijze kunnen uitdraaien van alle persoonsgegevens van een betrokkene die in een applicatie voorkomen, wanneer de betrokken daar om vraagt;
- de mogelijkheid inbouwen dat persoonsgegevens na verloop van een bepaalde periode automatisch verwijderd worden, of in ieder geval het systeem laten waarschuwen dat de bewaartermijn verstreken is;

- er aan de poort voor te zorgen dat de instellingen van systemen waarbij gevoelige persoonsgegevens worden verwerkt zodanig zijn dat de optie 'benaderbaar voor alle medewerkers' ontbreekt;
- het proces aanpassen zodat een ID alleen getoond behoeft te worden en geen kopie ID wordt bewaard.

Privacy by default
Privacy by default houdt in dat de gemeente technische en organisatorische maatregelen moet nemen om ervoor te zorgen dat, als standaard, alléén persoonsgegevens verwerkt die noodzakelijk zijn voor het specifieke doel dat moet worden bereikt. Bijvoorbeeld:
- een app niet de locatie van gebruikers te laten registeren als dat niet nodig is;
- op de website het vakje 'Ja, ik wil aanbiedingen ontvangen' niet vooraf aan te vinken;
- persoonsgegevens niet met collega's delen wanneer daarvoor geen noodzaak is.

De uitwerking van deze werkwijze wordt meegenomen in het nog te ontwikkelen proces voor privacy by design.

Data protection impact assessment
Een Data protection impact assessment (DPIA) is een instrument om vooraf de privacyrisico's van een gegevensverwerking in kaart te brengen. En vervolgens maatregelen te kunnen nemen om de risico's te verkleinen. Is hiervoor geen garantie te geven, dan moeten HLTsamen of de afzonderlijke gemeenten, de toezichthouder (AP) verplicht om advies vragen voordat de persoonsgegevens worden verwerkt. HLTsamen en de afzonderlijke gemeenten moeten dus zelf bepalen of er sprake is van een risicovolle verwerking. Daartoe wordt een methode ontwikkeld om periodiek risico-analyses te maken, te bepalen welke DPIA's noodzakelijk en urgent zijn en deze uit te voeren. Als 0-meting houden HLTsamen of de afzonderlijke gemeenten privacy-risicosessies op een aantal risicovolle onderdelen van de organisatie. De uitkomsten van deze risicosessies gebruikt het bestuursorgaan om te bepalen op welke verwerkingen een DPIA wordt toegepast. Voor de DPIA's wordt gebruik gemaakt van het model van de IBD. De Domein- en Teammanagers zijn verantwoordelijk voor de uitvoering van de DPIA. De FG adviseert over het uitvoeren van en de uitgevoerde DPIA's.
De AVG noemt drie categorieën verwerkingen waarin een DPIA in ieder geval moet worden uitgewerkt:
- systematische, uitgebreide en geautomatiseerde beoordeling van persoonlijke aspecten van de betrokkenen (bv profilering);
- grootschalige verwerking van bijzondere of strafrechtelijke gegevens;
- stelselmatige en grootschalige monitoring van openbaar toegankelijke ruimten.

De Autoriteit Persoonsgegevens heeft daarnaast een lijst van soorten verwerkingen opgesteld, waarvoor het uitvoeren van een DPIA verplicht is vóórdat met verwerken begonnen wordt. Deze lijst is niet uitputtend. Iedere keer dient zelf een afweging gemaakt te worden of het uitvoeren van de DPIA vereist is. De volgende informatie kan daarbij behulpzaam zijn: https://www.autoriteitpersoonsgegevens.nl/nl/zelf-doen/data-protection-impact-assessment-dpia#voor-welke-soorten-verwerkingen-is-het-uitvoeren-van-een-dpia-verplicht-6667

6. Organisatie
Inrichting en beschrijving van rollen met betrekking tot privacy:

Verantwoordelijk	**Rol**
Eindverantwoordelijk	De afzonderlijke Colleges van B&W, de burgemeesters en het bestuur van werkorganisatie HLTsamen
Feitelijk verantwoordelijk	Directieteam HLTsamen
Uitvoerend	Managementteam, Domein-en Teammanagers, privacycontactpersoon
Adviserend	Privacyofficer (PO) Functionaris gegevensbescherming (FG) Chief information security officer (CISO)
Geïnformeerd	FG, Gemeenteraden afzonderlijke gemeenten, Belanghebbenden/betrokkenen

In bijlage 3 zijn de verantwoordelijkheden en rollen in een tekening weergeven.

Gemeenteraden
De Gemeenteraden van de drie afzonderlijke gemeenten stellen de gemeentebrede kaders voor privacy en gegevensverwerking vast, inclusief de daarbij horende middelen. De gemeenteraden controleren het College van B&W bij de uitvoering van deze kaders en worden hiertoe in staat gesteld door de verantwoordingsinformatie die de afzonderlijke colleges van B&W en het bestuur van werkorganisatie

HLTsamen verschaffen. De gemeenteraden zijn daarnaast zelf verantwoordelijk voor het borgen van de privacy binnen hun griffie en de door hen ingestelde commissies.

De burgemeesters
De burgemeesters van de afzonderlijke gemeenten zijn voorzover het hun taakuitoefening betreft verantwoordelijk voor de naleving van de beginselen voor verwerking van persoonsgegevens en de maatregelen om te waarborgen en te kunnen aantonen dat de verwerking in overeenstemming met de AVG wordt uitgevoerd.

Colleges van B&W
De Colleges van B&W van de afzonderlijke gemeenten zijn integraal verantwoordelijk voor zorgvuldigheid van verwerking van (persoons-)gegevens. De Colleges van B&W van de afzonderlijke gemeenten leggen jaarlijks verantwoording af aan hun gemeenteraad over de realisatie en de toepassing van het privacybeleid in relatie tot het Informatiebeveiligingsbeleid, via de paragraaf bedrijfsvoering in de jaarstukken.

Het bestuur van HLTsamen
Het bestuur van HLTsamen is verantwoordelijk voor het inrichten van de privacyorganisatie. Zij is naar de organisatie en medewerkers kaderstellend en sturend en monitort de uitvoering van beleid. Het bestuur van HLTsamen stelt specifieke regelingen en procedures vast en draagt zorg voor het tijdig periodiek evalueren en bijstellen van het beleid. Het bestuur van HLTsamen stelt een procedure vast voor het melden met datalekken aan de Autoriteit Persoonsgegevens. Binnen het bestuur van HLTsamen wordt een portefeuillehouder privacy aangewezen.

Directie en managementteam HLTsamen
Het directieteam is voor het bestuur van HLTsamen ambtelijk opdrachtnemer en is eindverantwoordelijk voor de uitvoering van taken van de werkorganisatie. Directie- en managementteam HLTsamen stimuleren gezamenlijk kennisvergaring en bewustwording bij medewerkers. De domein- en teammanagers zien toe op de feitelijke uitvoering hiervan. De domein- en teammanagers zijn verantwoordelijk voor het intern melden van datalekken bij het datalekteam en de eventuele communicatie richting inwoners en betrokkenen[1]. Het directieteam is verantwoordelijk voor het besluit om het datalek te melden bij de Autoriteit Persoonsgegevens. Het feitelijk melden vindt plaats door Privacyofficer. De Functionaris Gegevensbescherming ziet erop toe op de uitvoering hiervan en voor de communicatie naar de Colleges van B&W.

Functionaris Gegevensbescherming (FG)
De verantwoordelijken (lees: het bestuur van HLTsamen en de bestuursorganen van de gemeenten Hillegom, Teylingen en Lisse) zijn verplicht een Functionaris Gegevensbescherming te benoemen (FG). De FG is onafhankelijk en kan op basis van artikel 37 AVG wat betreft de uitoefening van zijn functie geen aanwijzingen ontvangen van de verantwoordelijke of van de organisatie die hem heeft benoemd. De FG is contactpersoon voor de Autoriteit Persoonsgegevens en houdt intern toezicht op de naleving van wetgeving en de opvolging van aanbevelingen uit Data protection impact assessments. De FG ondersteunt het management bij het uitvoeren van de meldingsplicht datalekken.
De FG rapporteert periodiek aan het directie en/of managementteam HLTsamen en rapporteert jaarlijks aan de Colleges van B&W en de Gemeenteraden.

Chief Information Security Officer (CISO)
De CISO houdt toezicht op de informatiebeveiliging en rapporteert hierover aan de afzonderlijke Colleges van B&W. Hij bewaakt de voortgang van aanbevelingen uit audits en andere onderzoeken en adviseert over het te voeren beleid.

Privacyofficer (PO)
De Privacyofficer ondersteunt en adviseert domein- en teammanagers en heeft de volgende taken:
- adviseert gevraagd en ongevraagd over het implementeren en borgen van privacy;
- beheert het register van verwerkingsactiviteiten;
- ondersteunt de vakafdelingen bij het maken van afspraken met externe partijen over de veilige omgang met persoonsgegevens in de vorm van verwerkingsovereenkomsten en gegevensuitwisselingsovereenkomsten;
- draagt zorg voor de periodieke interne verantwoording richting de FG;
- functioneert als contactpersoon richting de FG;
- het toetsen van de processen naar de geldende privacynormen;
- het actueel houden van het register van verwerkingsactiviteiten;
- behandelt verzoeken van betrokkenen om inzage/afschrift, correctie, verwijdering en/of bezwaar;

1) Medewerkers zijn allen zélf verantwoordelijk voor het melden van incidenten. Bij de eventuele communicatie richting inwoners en betrokkenen kunnen ze (managers) uiteraard wél een rol spelen.

- verzorgt de feitelijke melding van datalekken bij de Autoriteit Persoonsgegevens.

Privacy contactpersoon (PC)
De domein- en teammanagers benoemen binnen de teams/domein een privacycontactpersoon. Een PM draagt zorg voor:
- het signaleren en melden van onjuist gebruik van persoonsgegevens bij de PO;
- het signaleren van organisatorische ontwikkelingen die verband houden met privacy- en informatiebeveiliging;
- het ondersteunen van de PO en de FG.

7. Implementatie en borging

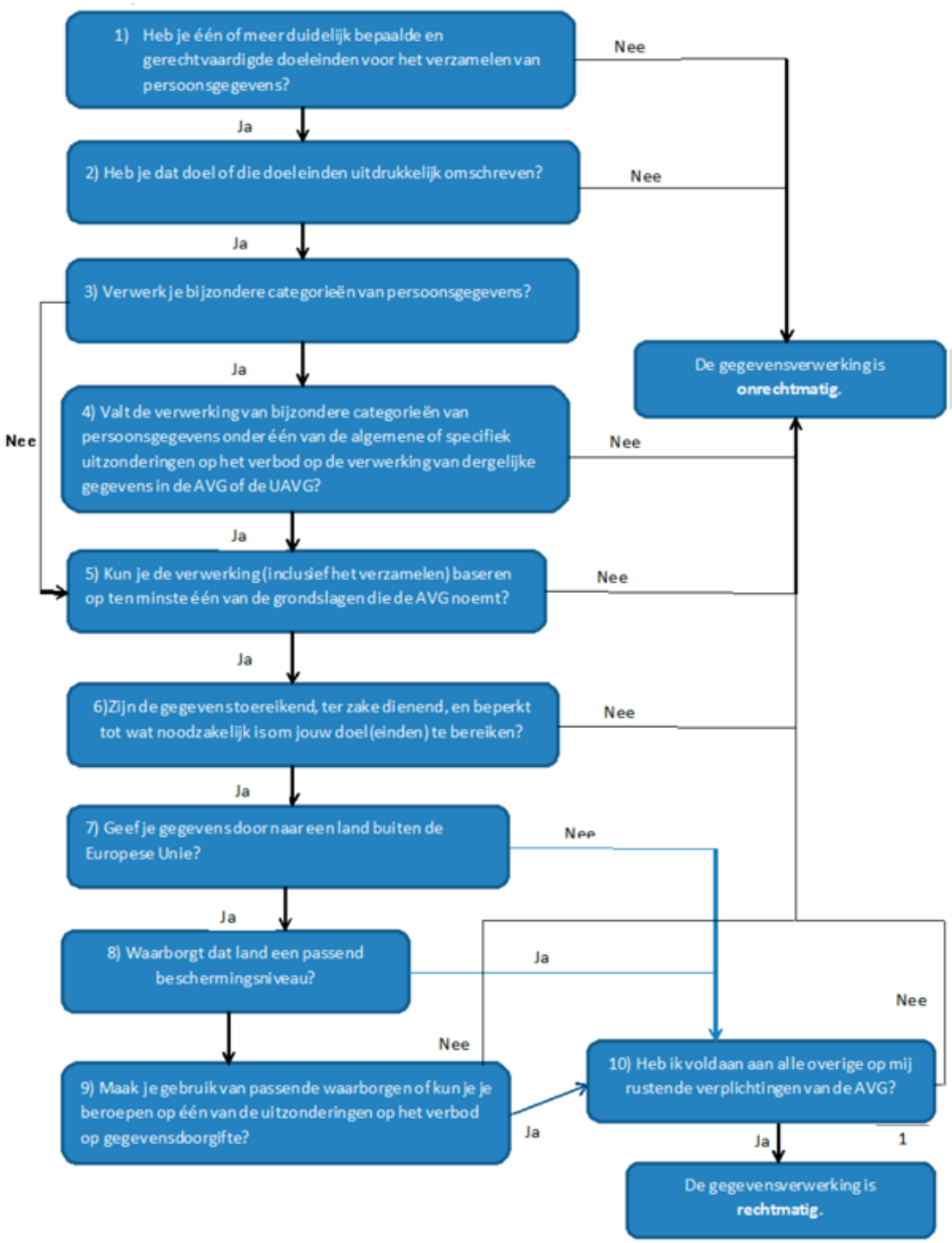
Uitgaande van het 10 stappenplan van de Autoriteit Persoonsgegevens voor implementatie van de AVG moeten de volgende acties uitgevoerd te worden:
- het inzichtelijk hebben en kunnen maken van alle gegevensverwerkingen (verwerkingenregister); de verwerkingen binnen de gemeente en HLTsamen zijn in kaart gebracht, maar voldoen nog niet aan alle vereisten uit de AVG.
- het maken van afspraken met derde partijen (o.a verwerkersovereenkomsten, gegevensuitwisselingsovereenkomsten).
- het creëren van bewustwording binnen de organisatie om de naleving van de AVG te vergroten.
- de inrichting van de procedures voor het uitoefenen van rechten; deze zijn nog niet formeel vastgesteld.
- het uitvoeren van DPIA's; er zijn thans drie DPIA's uitgevoerd: op toegang Wmo, het Informatiecentrum (registratie klantcontact) en cameratoezicht.
- het toepassen van Privacy-by-design en Privacy-by-default.
- het inregelen van de toestemmingsprocedure.
- het formaliseren van de procedure voor het melden van datalekken; er bestaat reeds een proces dat in de praktijk voldoet, maar dit is nog niet formeel vastgesteld.

Op 10 januari 2019 is het project "Grip op naleving Privacyregels" (hierna: project) van start gegaan. De verwachtte doorlooptijd is 9 maanden.
Binnen dit project worden concreet de volgende zaken opgeleverd:
- een juridisch getoetst verwerkingenregister;
- documenten om te ondersteunen bij de naleving;
- een privacybeleid;
- geactualiseerde 'Verordeningen verstrekking gegevens basisregistratie personen';
- presentaties binnen de ambtelijke organisatie om bewustzijn en naleving te vergroten;
- ambtelijke begeleiding oordeels- en besluitvorming betrokken besturen.

De werkorganisatie HLTsamen faciliteert de besturen van Hillegom, Teylingen en Lisse bij het vervullen van hun wettelijke taken. De werkzaamheden zijn ondergebracht in zes domeinen: Buitenruimte, Publiekservice, Bedrijfsvoering, Maatschappelijke ontwikkeling, Ruimtelijke ontwikkeling en Strategie en Projecten.

Op het vlak van gegevensbescherming kunnen sommige domeinen gemakkelijker voldoen aan de wettelijke eisen dan anderen. Dit hangt af in hoeverre sectorale wetgeving de Europese en nationale wetgeving op het vlak van gegevensbescherming inkleurt. Bovendien zijn de domeinen onderling verschillend georganiseerd. Het is te verwachten dat er verschillen in privacy-implementatie bestaan tussen de domeinen. Zolang de gemeente aan het maatschappelijk verkeer verantwoording aflegt, mag dat ook. Wel moet gewaakt worden dat rollen en taken voor gegevensverwerking niet zodanig worden belegd dat de verantwoordelijkheid voor de betrokken domeinen en teams weliswaar formeel is afgedekt, maar de naleving voor de organisatie als geheel onvoldoende is geborgd.

Bijlage 1. Stroomschema rechtmatige verwerking



Bijlage 2. Rechten betrokkenen

Burgers/medewerkers van HLTsamen hebben de volgende rechten[2]:

Rechten op inzage/afschrift

1. Het staat diegene, die betrokken is bij een gegevensverwerking van HLTsamen, vrij om inzage in de betreffende persoonsgegevens te vragen en om een afschrift van deze persoonsgegevens te verzoeken.
2. Het verzoek beschrijft specifiek hetgeen de betrokkene van HLTsamen aan inzage, of afschrift verlangt.
3. Een verzoek, als bedoeld in lid 1, kan door een betrokkene, of zijn gemachtigde, na identificatie worden ingediend door het invullen van het betreffende formulier aan één van de publieksbalies van HLTsamen of door het invullen van een e-formulier.
4. Een verzoek, als bedoeld in lid 1, wordt in beginsel binnen één maand afgehandeld. HLTsamen behoudt zich het recht voor genoemde termijn éénmalig met twee maanden te verlengen.

Recht op correctie

1. Het staat diegene, die betrokken is bij een gegevensverwerking van HLTsamen, vrij om correctie van de eigen persoonsgegevens te vragen.
2. Het verzoek beschrijft zowel de foutieve persoonsgegevens evenals de juiste persoonsgegevens.
3. Een verzoek, als bedoeld in lid 1, kan door een betrokkene, of zijn gemachtigde, na identificatie worden ingediend door het invullen van het betreffende formulier aan één van de publieksbalies van HLTsamen of door het invullen van een e-formulier.
4. Een verzoek, als bedoeld in lid 1, wordt in beginsel binnen één maand afgehandeld. HLTsamen behoudt zich het recht voor genoemde termijn éénmalig met twee maanden te verlengen.

Recht op verwijdering

1. Het staat diegene, die betrokken is bij een gegevensverwerking van HLTsamen, vrij om een verwijderingsverzoek persoonsgegevens in te dienen.
2. Een verwijderingsverzoek persoonsgegevens wordt toegewezen indien:
   a. de bewaar- en vernietigingstermijnen zijn verstreken;
   b. de betrokkene zijn expliciet gegeven toestemming herroept;
   c. de persoonsgegevens onrechtmatig zijn verwerkt.
3. Een verzoek, als bedoeld in lid 1, kan door een betrokkene, of zijn gemachtigde, na identificatie worden ingediend door het invullen van het betreffende formulier aan één van de publieksbalies van HLTsamen of door het invullen van een e-formulier.
4. Een verzoek, als bedoeld in lid 1, wordt in beginsel binnen één maand afgehandeld. HLTsamen behoudt zich het recht voor genoemde termijn éénmalig met twee maanden te verlengen.

Recht op bezwaar

1. Het staat diegene, die betrokken is bij een gegevensverwerking van HLTsamen, vrij om bezwaar in te dienen tegen een verwerking van persoonsgegevens.
2. De betrokkene beargumenteert waarom een bepaalde gegevensverwerking onverenigbaar is met het beoogde verwerkingsdoel.
3. Een verzoek, als bedoeld in lid 1, kan door een betrokkene, of zijn gemachtigde, na identificatie worden ingediend door het invullen van het betreffende formulier aan één van de publieksbalies van HLTsamen of door het invullen van een e-formulier.
4. Een verzoek, als bedoeld in lid 1, wordt in beginsel binnen één maand afgehandeld. HLTsamen behoudt zich het recht voor genoemde termijn éénmalig met twee maanden te verlengen.

Weigeringsgronden en rechtsbescherming

1. HLTsamen weigert een verzoek om een recht op inzage/afschrift, recht op correctie en recht op verwijdering, indien:
   a. de identiteit van de verzoeker niet kan worden vastgesteld;
   b. het verzoek inbreuk maakt op de rechten en vrijheden van anderen;
   c. het verzoek, gelet op de daaraan voorafgaande verzoeken, door een betrokkene met onredelijke tussenpozen wordt ingediend.
2. Tegen een schriftelijke beslissing op een verzoek om een recht op inzage/afschrift, recht op correctie en recht op verwijdering, staat bezwaar en beroep in de zin van de Algemene wet bestuursrecht open.

2) Bij het afhandelen van de verzoeken wordt vooraf zoveel mogelijk de informele aanpak gevolgd.

Bijlage 3. Verantwoordelijkheden en rollen schematisch Schema aanpassen