gemeente Lelystad

GEMEENTEBLAD

Officiële uitgave van de gemeente Lelystad

Nr. 250938

11 juni

2025

Strategisch beleid informatiebeveiliging en privacy 2025 – 2028

1. Inleiding

Deze beleidsnota beschrijft het strategisch informatiebeveiligings- en privacybeleid voor de jaren 2025 tot en met 2028 en vervangt het in 2023 vastgestelde 'Gemeentelijk Informatiebeveiligingsbeleid 2023-2025' en het in 2018 vastgestelde privacybeleid.
Dit document bevat het strategisch Informatie- en privacy beleid en is daarmee richtinggevend en kaderstellend voor alle andere aanvullende beleidsdocumenten, procedures en standaarden van de gemeenten. Het strategisch beleid wordt aangevuld met onderwerp specifieke beleidsdocumenten voor informatiebeveiliging op tactisch niveau en werkinstructies op operationeel niveau. Op privacyniveau geeft het privacyreglement hier verder invulling aan; zie bijlage Privacyreglement onder aan dit beleidsdocument.

Ten opzichte van voorgaand beleid, is in deze versie het beleid rondom informatiebeveiliging en privacy samengevoegd en sluit deze aan bij het algemene informatiebeleid om ervoor te zorgen dat zowel de gegevens als de bedrijfsdoelen goed beschermd zijn.
Met dit 'Strategisch beleid Informatiebeveiligingsbeleid en privacy 2025 t/m 2028' wil de gemeente de beveiliging van persoonsgegevens en andere informatie binnen de gemeente continueren en voortgaan op de stappen die in de voorgaande jaren gezet zijn. De basis voor dit strategisch beleid is de NEN-ISO/IEC 27001/27002 en de daarvan afgeleide Baseline Informatiebeveiliging Overheid (BIO[1]) en het VNG Borgingsproduct AVG versie 3.0[2]. De principes die zijn gehanteerd bij het opstellen van dit strategisch beleid, zijn gebaseerd op de 10 bestuurlijke principes voor informatiebeveiliging[3] zoals uitgewerkt door de VNG en de beginselen uit de AVG voor het verwerken van persoonsgegevens[4]

1.1 Leeswijzer

In hoofdstuk 2 wordt de kern van het strategisch beleid uiteengezet. Dit beleid wordt op tactisch en operationeel niveau aangevuld met onderwerp specifieke tactische beleidsregels die invulling geven op dit strategisch beleid. In het jaarlijks uit te brengen gemeentelijk Informatiebeveiligings- en privacy plan worden deze tactische en operationele aspecten van de informatiebeveiliging en privacy verder uitgewerkt en geconcretiseerd. Dit wordt gedaan op basis van input van de teamleiders, de CISO, ISO, de privacyfunctionarissen (PO en FG), het dreigingsbeeld van de IBD en de uitkomsten van ENSIA, risicoanalyses en DPIA's. Daarin staan dan ook de acties en planning vermeld, om de praktijk in overeenstemming te brengen met datgene wat in het beleid is geëist. Hoofdstuk 3 beschrijft vervolgens hoe de taken en verantwoordelijkheden in de organisatie belegd zijn.

1.2 Informatiebeveiliging

Onder informatiebeveiliging wordt verstaan het treffen en onderhouden van een samenhangend pakket van maatregelen om de betrouwbaarheid van de informatievoorziening aantoonbaar te waarborgen. Kernpunten daarbij zijn beschikbaarheid, integriteit en vertrouwelijkheid van persoonsgegevens en andere informatie.
Het informatiebeveiligingsbeleid geldt voor alle processen van de gemeente en borgt daarmee de informatievoorziening gedurende de hele levenscyclus van informatiesystemen, ongeacht de toegepaste technologie en ongeacht het karakter van de informatie. Het beperkt zich niet alleen tot de ICT en heeft betrekking op het politieke bestuur, alle medewerkers, burgers, gasten, bezoekers, ICT-dienstenleveranciers, ketenpartners en externe relaties.

1.3 Privacy & Gegevensbescherming (AVG)

De gemeente werkt met (persoons)gegevens van inwoners, ondernemers, medewerkers en (keten)partners. Deze gegevens verzamelt de gemeente voor het goed kunnen uitvoeren van de gemeentelijke wettelijke taken. Denk hierbij onder andere aan taken in het sociaal domein, openbare orde en veiligheidsdomein of voor burgerzaken. Om als gemeente deze taken goed uit te voeren zijn persoonsgegevens noodzakelijk.

1) Link naar BIO2 – Informatiebeveiligingsdienst
2) Link naar AVG Borgingsproduct 3.0 – Informatiebeveiligingsdienst
3) Link naar De 10 bestuurlijke principes voor informatiebeveiliging – Informatiebeveiligingsdienst
4) Link naar Grondslagen AVG uitgelegd - Autoriteit Persoonsgegevens

Bij de omgang met persoonsgegevens van inwoners en personeel hebben gemeenten een grote verantwoordelijkheid. Privacy is een essentieel en complex vraagstuk. Dit komt onder andere door de toenemende digitalisering van de samenleving en dienstverlening van gemeenten, de decentralisatie van overheidstaken naar gemeenten, de gegevensuitwisseling met (keten)partners, de technische mogelijkheden en veranderende wetgeving. Privacy raakt de hele gemeentelijke organisatie en verdient, samen met informatiebeveiliging, continu aandacht. De inwoner moet erop kunnen vertrouwen dat de gemeente zorgvuldig en veilig met deze persoonsgegevens omgaat.

1.4 Visie, Ambitie en Doelstellingen van de gemeente op het gebied van informatieveiligheid
Visie en Ambitie:
Een betrouwbare informatievoorziening is noodzakelijk voor het goed functioneren van de gemeente en de basis voor het beschermen van rechten van burgers en bedrijven. Zeker nu we in een wereld leven waarin we steeds meer afhankelijk zijn van digitale technologie en het internet, is daarmee de noodzaak voor informatiebeveiliging groter dan ooit. Een visie op informatiebeveiliging moet daarom gericht zijn op het beschermen van de digitale infrastructuur en gegevens van een organisatie tegen cyberdreigingen. In het raadsakkoord is cyberveiligheid als speerpunt opgenomen.

Ons doel is om een veilige digitale omgeving te creëren waar informatiebeveiliging geïntegreerd is in onze dagelijkse werkzaamheden en processen. Hierdoor zullen we de continuïteit van onze bedrijfsvoering verhogen, de vertrouwelijkheid, integriteit en beschikbaarheid van onze gegevens beschermen.

Een belangrijk onderdeel daarbij is het creëren van **bewustzijn onder medewerkers** over de risico's en cyberdreigingen en hoe ze hiermee om kunnen gaan. We zetten informatiebeveiliging hoog op de agenda en gaan onze medewerkers bijscholen, trainen en inhoudelijk ondersteunen.

Vanuit de cyberbeveiligingswet is het aan de gemeente om te **voldoen aan de standaard** van informatiebeveiliging basisnormenkader **Baseline Informatiebeveiliging Overheid** (BIO2) in opzet, bestaan en werking van beheersmaatregelen. Gemeente Lelystad conformeert zich hieraan.

We willen onze organisatie beschermen tegen cyberbedreigingen en daarmee een bijdrage leveren aan een veilige digitale samenleving. We **borgen daarbij de preventieve fase** (firewall, encryptie en beveiligingssoftware) en **zetten in op** detectieve en repressieve maatregelen. Daarmee bedoelen we, **snelheid van signaleren en snelheid van herstel** bij calamiteiten.

We zullen onze beveiligingsgegevens periodiek **evalueren en bijstellen** om ons aan te passen aan de veranderende cyberdreigingen en de vereiste wet- en regelgeving.

Dit strategisch informatiebeveiligingsbeleid geeft hier de kaders voor aan. Het tactisch informatiebeveiligingsbeleid zorgt voor praktische handvatten om te komen van doel naar actie.
De BIO beschrijft vervolgens de benodigde maatregelen voor zowel Mens (gedrag), Proces en Techniek op de te beschermen informatie.

Strategische doelen:
Naast een verhoogde weerbaarheid en een hoger volwassenheidsniveau draagt deze visie en ambitie ook bij aan:
- Het managen van de informatiebeveiliging.
- Adequate bescherming van bedrijfsmiddelen en persoonsgegevens.
- Het toepassen van dataminimalisatie.
- Het minimaliseren van risico's van menselijk gedrag.
- Het voorkomen van ongeautoriseerde toegang.
- Het garanderen van correcte en veilige informatievoorzieningen.
- Het beheersen van de toegang tot informatiesystemen.
- Het waarborgen van veilige informatiesystemen.
- Het adequaat reageren op incidenten.
- Het beschermen van (kritieke) bedrijfsprocessen.
- Het beschermen en correct verwerken van persoonsgegevens van burgers en medewerkers.
- Voldoen aan de wettelijke verplichtingen voortvloeiend uit de AVG en Cyberbeveiligingswet en dit op ieder moment met bewijs kunnen aantonen.
- Het waarborgen van de naleving van dit beleid.

Totstandkoming:
Om tot deze visie te komen, hebben zowel interne alsook externe factoren bijgedragen, namelijk:
- Wet Cyberbeveiliging
- Het raadsakkoord uit 2022

- Lelystad op koers 2030
- Projecten binnen LD2025
- De cloud-strategie
- Dreigingsbeeld 2023-2024
- Toename aantal ketenpartners
- Toenemende wet- &regelgeving
- Toenemende (wettelijk verplichte) verantwoording aan ministeries, ketenpartners en inwoners
- Input TL IMA, CIO en Directeur Bedrijfsvoering
- Consultatiereactie BIO2 vanuit de VNG aan MINBZK

Tot slot:
Middels dit beleid en het beleggen van ambtelijke- en bestuursverantwoordelijkheid, wordt vormgegeven aan een strategische aanpak van informatiebeveiliging. Zowel het College van B&W, de Directie (DT) en de proceseigenaren (teamleiders) zullen op basis van risicomanagement bewuste keuzes moeten maken om informatieveiligheid volgens de BIO te borgen en om kwetsbaarheden in de bedrijfsvoering te mitigeren (beheersen, vermijden, overdragen of accepteren). En hebben daarbij een voorbeeldfunctie.

1.5 Visie, Ambitie en Doelstellingen van de gemeente op het gebied van privacy
Visie en ambitie:
De gemeente streeft ernaar om het vertrouwen van haar inwoners, burgers en (keten)partners te behouden door te zorgen voor een transparante, veilige en verantwoorde omgang met persoonsgegevens. Privacy is een fundamenteel recht, en de gemeente ziet het als haar plicht om dit recht te beschermen in al haar processen en diensten. Dit betekent dat de gemeente handelt volgens de hoogste normen van gegevensbescherming, in overeenstemming met wet- en regelgeving, en voortdurend streeft naar verbetering in de bescherming van persoonsgegevens.

De gemeente gaat mee met de nieuwste ontwikkelingen. Innovatieve voorzieningen, globalisering en een steeds meer digitale overheid stellen andere eisen aan de bescherming van gegevens en privacy. De gemeente is zich hiervan bewust en zorgt dat de privacy gewaarborgd blijft, onder andere door maatregelen op het gebied van informatiebeveiliging, dataminimalisatie, transparantie en gebruikerscontrole. Het bestuur en management spelen een cruciale rol bij het waarborgen van privacy. De gemeente Lelystad geeft middels dit beleid een duidelijke richting aan privacy en laat zien dat zij de privacy waarborgt, beschermt en handhaaft. Dit beleid is van toepassing op de gehele organisatie, alle processen, onderdelen, objecten en gegevensverzamelingen van de gemeente. Dit privacybeleid van gemeente Lelystad is in lijn met het algemene beleid van de gemeente en de relevante lokale, regionale, nationale en Europese wet- en regelgeving.

De gemeente heeft de ambitie om een voorbeeld te zijn op het gebied van privacybescherming door:
- ***Transparantie en Verantwoording:*** zich openlijk en duidelijk uit te spreken over hoe en waarom persoonsgegevens worden verzameld, gebruikt en bewaard. Dit omvat het informeren van inwoners over hun rechten en het verstrekken van duidelijke en begrijpelijke informatie over het privacybeleid.
- ***Veiligheid en Vertrouwelijkheid:*** het implementeren van robuuste technische en organisatorische maatregelen om persoonsgegevens te beschermen tegen ongeautoriseerde toegang, verlies of misbruik. Dit omvat het up-to-date houden van beveiligingssystemen en het regelmatig uitvoeren van audits en risicoanalyses.
- ***Continue Verbetering:*** doorlopend werken aan de verbetering van privacybescherming door het volgen van technologische ontwikkelingen, wetenschappelijke inzichten en maatschappelijke behoeften. De gemeente stelt zich flexibel op om te anticiperen op nieuwe uitdagingen en om in te spelen op veranderende wetgeving.
- ***Cultuur en Bewustzijn:*** het bevorderen van een privacybewuste cultuur binnen de gehele organisatie, door middel van trainingen, communicatie en het stimuleren van een 'privacy by design' aanpak bij het ontwikkelen van nieuwe diensten en processen.

Hiermee wil de gemeente niet alleen voldoen aan de wet- en regelgeving, maar ook het vertrouwen en de tevredenheid van haar inwoners versterken en behouden.

*De gemeente houdt zich hierbij aan de volgende **doelstellingen**:*
- *Rechtmatigheid, behoorlijkheid, transparantie*
  Persoonsgegevens worden in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze verwerkt.
- *Grondslag en doelbinding*
  De gemeente zorgt ervoor dat persoonsgegevens alleen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doelen worden verzameld en verwerkt. Persoonsgegevens worden alleen met een rechtvaardige grondslag verwerkt.

- *Dataminimalisatie*
  De gemeente verwerkt alleen de persoonsgegevens die minimaal noodzakelijk zijn voor het vooraf bepaalde doel. De gemeente streeft naar minimale gegevensverwerking. Waar mogelijk worden minder of geen persoonsgegevens verwerkt.
- *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. Teams stellen zich op de hoogte van de bewaartermijn en bewaken de bewaartermijn.
- *Integriteit en vertrouwelijkheid*
  De gemeente gaat zorgvuldig om met persoonsgegevens en behandelt deze vertrouwelijk. Zo worden persoonsgegevens alleen verwerkt door personen met een geheimhoudingsplicht en voor het doel waarvoor deze gegevens zijn verzameld. Daarbij zorgt de gemeente voor passende beveiliging van persoonsgegevens. Deze beveiliging is vastgelegd in het informatiebeveiligingsbeleid.

- *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. De gemeente controleert deze afspraken periodiek.
- *Subsidiariteit*
  Voor het bereiken van het doel waarvoor de persoonsgegevens worden verwerkt, wordt inbreuk op de persoonlijke levenssfeer van de betrokken burger zoveel mogelijk beperkt.
- *Proportionaliteit*
  De inbreuk op de belangen van de betrokkene mag niet onevenredig zijn in verhouding tot en met de verwerking te dienen doel.
- *Rechten van betrokkenen*
  De gemeente honoreert alle rechten van betrokkenen op grond van de AVG

Wettelijke kaders voor de omgang met gegevens
De gemeente is verantwoordelijk voor het opstellen, uitvoeren en handhaven van het beleid. Hiervoor gelden onder andere de volgende wettelijke kaders:
- Algemene Verordening Gegevensbescherming (AVG)
- Uitvoeringswet Algemene Verordening Gegevensbescherming
- Cyberbeveiligingswet
- Wet politiegegevens (Wpg) (Boa's die voor handhavingstaken persoonsgegevens verwerken)
- Sectorale wetgeving zoals WMO, Jeugdwet
- Archiefwet

2. Strategisch beleid

2.1 Algemeen

Een betrouwbare informatievoorziening is essentieel voor het goed functioneren van de processen bij de gemeente. Informatiebeveiliging is het proces dat deze betrouwbare informatievoorziening borgt. Het opnemen van informatiebeveiliging als normaal kwaliteitscriterium voor een gezonde bedrijfsvoering is tegenwoordig niet langer een keuze, maar bittere noodzaak geworden.

Het doel van deze beleidsnota is het presenteren van het "Strategisch Informatiebeveiligings- en privacybeleid 2025 - 2028". De uitwerking van dit beleid in concrete maatregelen en activiteiten vindt plaats in het jaarlijks bij te stellen informatiebeveiligings- en privacyplan (IB&P-P). Het beleid op informatiebeveiliging en privacy dient ondersteuning te bieden aan het bestuur, het management en de organisatie bij de sturing op en het beheer van informatieveiligheid en privacy.

En daarmee draagt dit beleid bij aan het uiteindelijke doel: Het borgen van betrouwbare dienstverlening en een aantoonbaar niveau van informatiebeveiliging dat
- Voldoet aan de relevante wetgeving
- Algemeen wordt geaccepteerd door haar (keten) partners en
- Er mede voor zorgt dat de kritische bedrijfsprocessen bij een calamiteit voortgezet kunnen worden.

Het informatiebeveiligings- en privacybeleid heeft een geldigheid van 3 jaar, wordt minimaal jaarlijks geëvalueerd en indien nodig eerder bijgesteld en opnieuw vastgesteld. Het vaststellen van het Privacybeleid is belegd bij het college van B&W. Daarom zal dit gezamenlijke beleid via het DT worden vastgesteld door het college van B&W. De meest actuele versie van het beleid is te vinden op www.lelystad.nl. In de bijlage van dit document is het privacyreglement opgenomen.

2.2 Ontwikkelingen

De ontwikkelingen die van belang zijn voor de actualisering van het informatiebeveiligings- en privacybeleid zijn de volgende:

2.2.1 De BIO

De BIO (Baseline Informatiebeveiliging Overheid) is het normenkader voor de gehele overheid. De werkwijze van deze BIO is gericht op risicomanagement. Dat wil zeggen dat de teamleiders nu meer dan vroeger moeten werken volgens de aanpak van de ISO 27001 en daarbij is risicomanagement van belang. Dit houdt voor het management in, dat men op voorhand keuzes maakt en continu afwegingen maakt of informatie in bestaande en nieuwe processen adequaat beveiligd zijn in termen van beschikbaarheid, integriteit en vertrouwelijkheid.

Risicomanagement
Informatiebeveiliging richt zich op het risico dat informatie niet op het juiste moment beschikbaar is, niet juist of volledig is of in verkeerde handen terecht kan komen. Proceseigenaren (teamleiders) zullen zich dus een beeld moeten vormen van de kwetsbaarheden in hun processen en systemen: hoe groot is de kans dat zo'n kwetsbaarheid wordt misbruikt en wat zijn de gevolgen (impact) daarvan? En aan de andere kant: met welke dreigingen moeten we rekening houden. Precies daar tussenin bevindt zich de vraag: welke maatregelen dient een eigenaar te treffen om de kwetsbare informatie beschermen tegen de kwaadwillenden. En juist daarom is risicomanagement de basis voor informatiebeveiliging, waar de teamleider beslist en de (C)ISO adviseert.

2.2.2 De AVG

Nieuwe technologische ontwikkelingen, innovatieve voorzieningen, globalisering en een steeds digitaler wordende overheid maakt het zorgvuldig omgaan met persoonsgegevens steeds complexer en noodzakelijker. De gemeente Lelystad is zich hiervan bewust en wil daarom met dit beleid aangeven hoe zij in algemene zin invulling geeft aan nationale en Europese wet- en regelgeving op het gebied van privacy, waaronder de Algemene Verordening Gegevensbescherming (hierna te noemen: AVG).

2.2.3 De WPG

De gemeente heeft BOA's in dienst en zij verwerken gegevens die niet onder de AVG vallen maar onder de wet Politiegegevens (WPG). Hiervoor moet de gemeentebeleid en samenhangende procedures hebben ingeregeld die betrekking hebben op toegangsrechten, autorisaties, data classificatie, risicoinschatting, registratie en logging, meldplicht en documentatieplicht

2.2.4 De 10 principes voor informatiebeveiliging en privacy[5]

De 10 principes voor informatiebeveiliging zijn een bestuurlijke aanvulling op het normenkader BIO en gaan over de waarden die de bestuurder zichzelf oplegt. De principes zijn als volgt:

1. Bestuurders bevorderen een veilige cultuur.
2. Informatiebeveiliging en privacy is van iedereen.
3. Informatiebeveiliging is risicomanagement.
4. Risicomanagement is onderdeel van de besluitvorming.
5. Informatiebeveiliging en privacy behoeft ook aandacht in (keten)samenwerking.
6. Informatiebeveiliging en privacy is een proces.
7. Informatiebeveiliging en privacy kost geld.
8. Onzekerheid dient te worden ingecalculeerd.
9. Verbetering komt voort uit leren en ervaring.
10. Het bestuur controleert en evalueert.

De principes gaan vooral over de rol van het bestuur bij het borgen van informatiebeveiliging en privacy in de gemeentelijke organisatie. Deze principes ondersteunen de bestuurder bij het uitvoeren van goed risicomanagement. Als er iets verkeerd gaat met betrekking tot het beveiligen van de informatie binnen de gemeentelijke processen, dan kan dit directe gevolgen hebben voor inwoners, ondernemers en partners van de gemeente. Daarmee is het onderwerp informatiebeveiliging en privacy nadrukkelijk gewenst op de bestuurstafel.

2.2.5 Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten

Het Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten geeft een actueel zicht op incidenten en factoren uit het verleden, aangevuld met een verwachting voor het heden en de nabije toekomst. Dit dreigingsbeeld is daarmee het ideale document om focus aan te brengen in het actualiseren van beleid en plannen voor informatiebeveiliging.

5) https://www.informatiebeveiligingsdienst.nl/product/de-10-bestuurlijke-principes-voor-informatiebeveiliging/

2.2.6 Informatie uit incidenten en inbreuken op de beveiliging en datalekken

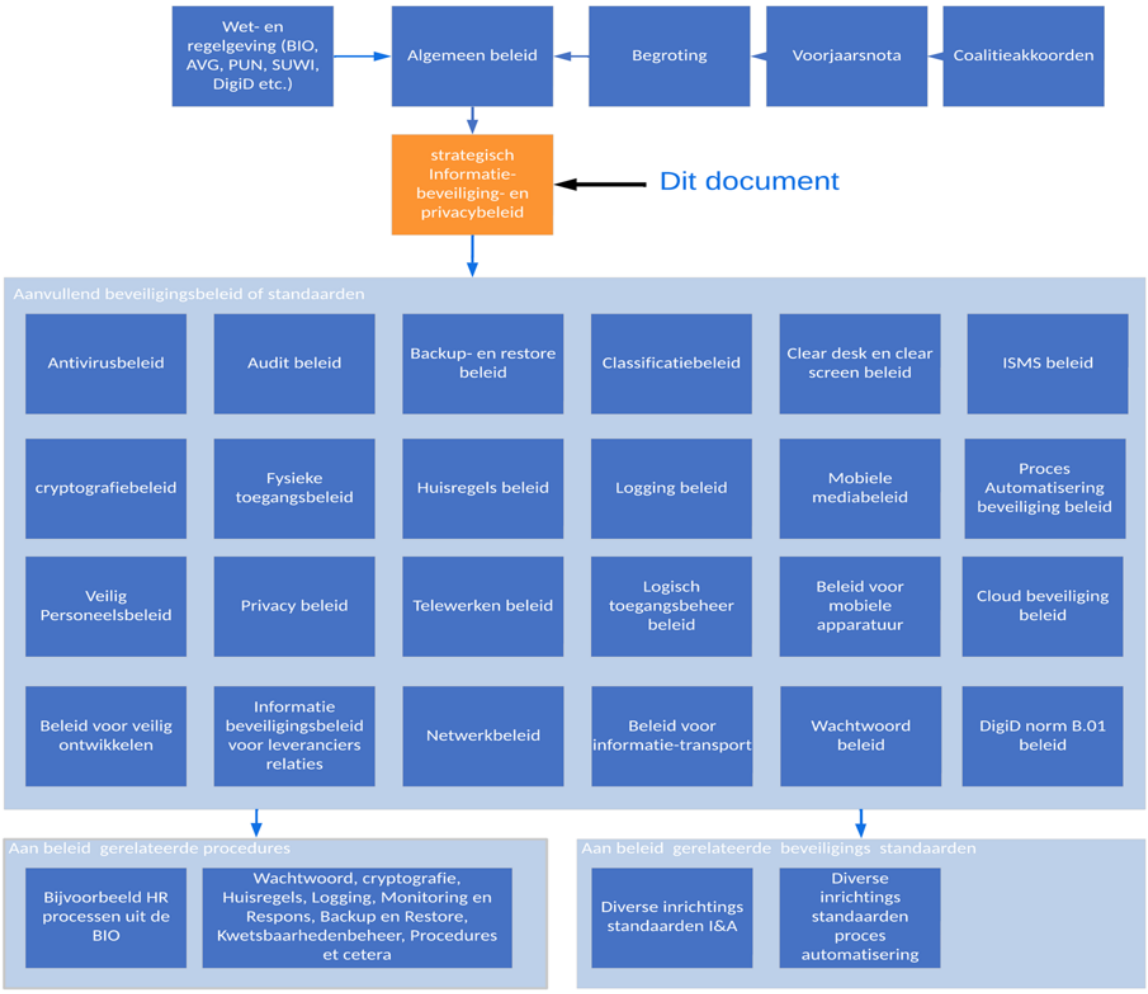
De gemeente kent naast het hierboven genoemde dreigingsbeeld natuurlijk een eigen systeem waarin incidenten worden vastgelegd. Dit systeem geeft ook waardevolle informatie om van te leren en dus zijn incidenten uit het verleden ook nadrukkelijk input bij het actualiseren van het beleid.

2.3 Standaarden informatiebeveiliging

Voor de ondersteuning van gemeenten bij het formuleren en realiseren van hun informatiebeveiligingsbeleid heeft de interbestuurlijke werkgroep Normatiek[6] in 2018 de Baseline Informatiebeveiliging Overheid (BIO) uitgebracht, afgeleid van de wereldwijd geaccepteerde beveiligingsnormen ISO 27001 en ISO 27002. Deze BIO bestaat uit een baseline met verschillende niveaus van beveiligen. De inhoud en structuur van deze beleidsnota zijn afgestemd op die van de BIO. Ook het Informatiebeveiligings- en privacyplan zal deze structuur volgen.
Binnen de gemeente wordt naast ICT ook Operationele Technologie (OT) ingezet. Met OT worden systemen bedoeld voor de besturing van apparaten voor middel van Proces Automatisering (PA). Het beveiligingsbeleid van de gemeente is ook voor de bescherming van PA van toepassing.

2.4 Plaats van het strategisch beleid

Het strategisch beleid wordt gebruikt om de basis te leggen voor de tactische beleidsplannen en daarmee richting te geven voor de verdere invulling van informatiebeveiliging en privacy op tactisch en operationeel niveau. Deze beleidsnota beschrijft op strategisch niveau het informatiebeveiligings- en privacy beleid. Dit beleid is vertaald in aanvullend beleid en tactische en operationele richtlijnen en maatregelen. De daaruit voortkomende werkzaamheden worden uitgewerkt in het jaarlijks te schrijven 'Gemeentelijk Informatiebeveiligings- en privacyplan'.



6) De Interbestuurlijke werkgroep Normatiek bestaat uit vertegenwoordigers van bijvoorbeeld VNG en de IBD, maar ook waterschappen, provincies en het rijk.

2.5 Scope informatiebeveiliging en privacy

De scope van dit beleid omvat alle gemeentelijke processen, onderliggende informatiesystemen, Operationele Technologie (OT), informatie (fysiek en digitaal) en gegevens(verzamelingen) van de gemeente, het gebruik daarvan door medewerkers en (keten)partners in de meest brede zin van het woord, ongeacht locatie, tijdstip en gebruikte apparatuur.

Dit strategisch gemeentelijke Informatiebeveiligingsbeleid is een algemene basis en dekt tevens aanvullende beveiligingseisen uit wetgeving af zoals voor de Cyberbeveiligingswet, AVG, UAVG, Wpg. Voor bepaalde kerntaken gelden op grond van wet- en regelgeving ook nog enkele specifieke (aanvullende) beveiligingseisen, bijvoorbeeld SUWI, gemeentelijke basisregistraties en DigiD. Deze worden in aanvullende (beleids)documenten geformuleerd.
Bewust wordt in het strategisch beleid geen uitputtend overzicht van onderliggende documenten opgenomen. In de onderliggende documenten wordt de link naar het strategisch beleid gelegd.

- Alle informatie en informatiesystemen zijn van belang voor de gemeente, bepaalde informatie is van vitaal en kritiek belang. Het college van B en W is eindverantwoordelijke voor de informatiebeveiliging en privacy. Dit geldt voor alle gemeentelijke informatiesystemen ongeacht waar deze worden gehost.
- Binnen de scope vallen daarbij ook alle Operationele Technologie (OT) die binnen de gemeentelijke gebouwen en in de publieke ruimte van de gemeente worden gebruikt, die van de gemeente zijn, zoals gebouwbeheersingssystemen en bijvoorbeeld camera technologie of pompen en gemalen.

2.6 Uitgangspunten

Het bestuur, het directieteam en de teamleiders spelen een cruciale rol bij het uitvoeren van dit strategische IB&P beleid. Het management maakt een inschatting van het belang dat de verschillende delen van de informatievoorziening voor de gemeente heeft, de (privacy)risico's die de gemeente hiermee loopt en welke van deze risico's onacceptabel hoog zijn.
Op basis hiervan zet het management dit beleid voor informatiebeveiliging en privacy op, draagt dit uit naar de organisatie en ondersteunt en bewaakt de uitvoering ervan.

Het gehele gemeentelijk management geeft een duidelijke richting aan informatiebeveiliging en privacy en demonstreert dat zij informatiebeveiliging en privacybescherming ondersteunt en zich hierbij betrokken voelt, door het uitdragen en handhaven van een IB&P beleid van en voor de hele gemeente. Dit beleid is van toepassing op de gehele organisatie, alle processen, organisatieonderdelen, objecten, informatiesystemen, Operationele Technologie (OT) en (persoons)gegevens(verzamelingen). Het IB&P beleid is in lijn met het algemene beleid van de gemeente en de relevante landelijke en Europese wet- en regelgeving.

2.6.1 Belangrijkste uitgangspunten

De belangrijkste uitgangspunten van het beleid zijn:

- De uitvoering van de informatiebeveiliging is een verantwoordelijkheid van het lijnmanagement. Alle informatiebronnen en -systemen (ICT/IoT/OT) die gebruikt worden door de gemeente Lelystad hebben een interne eigenaar die de vertrouwelijkheid, privacy eisen en/of waarde bepaalt van de informatie die ze bevatten. De primaire verantwoordelijkheid voor de bescherming van informatie ligt dan ook bij de eigenaar van de informatie.
- Door periodieke controle, organisatiebrede planning én coördinatie wordt de kwaliteit van de informatievoorziening en privacy verankerd binnen de organisatie. Het IB&P beleid vormt samen met het IB&P plan het fundament onder een betrouwbare informatievoorziening en privacybescherming. In het IB&P plan wordt de betrouwbaarheid van de informatievoorziening en privacy organisatiebreed benaderd. Het plan wordt periodiek bijgesteld op basis van nieuwe ontwikkelingen, registraties in het incidentenregister en risicoanalyses voor informatiebeveiliging en privacy.
- Informatiebeveiliging en privacybescherming is een continu verbeterproces. 'Plan, do, check en act' vormen samen het managementsysteem van informatiebeveiliging en privacybescherming.
- De gemeente stelt de benodigde mensen en middelen beschikbaar om haar eigendommen en werkprocessen te kunnen beveiligen en te voldoen aan de privacy eisen volgens de wijze zoals gesteld in dit beleid.
- Regels en verantwoordelijkheden voor het IB&P beleid dienen te worden vastgelegd en vastgesteld. (Zie hoofdstuk 3)
- Iedere medewerker, zowel vast als tijdelijk, intern of extern, is verplicht waar nodig gegevens en informatiesystemen te beschermen tegen ongeautoriseerde toegang, gebruik, verandering, openbaring, vernietiging, verlies of overdracht en bij vermeende inbreuken hiervan melding te maken.

- Het borgen van privacy in de uitvoering van gemeentelijke processen vindt risico gestuurd plaats. De verantwoordelijken in de organisatie maken afwegingen ter naleving van privacyregels en op basis van een risico-inschatting.

2.6.2 Randvoorwaarden

Belangrijke randvoorwaarden zijn:

- De informatiebeveiliging en privacy eisen maken deel uit van afspraken met ketenpartners, leveranciers en gemeenschappelijke regelingen en worden periodiek geëvalueerd/gecontroleerd.
- Kennis en bewustzijn van informatiebeveiliging en privacybescherming en omgaan met persoonsgegevens binnen de organisatie dienen actief bevorderd en geborgd te worden.
- Jaarlijks wordt een informatiebeveiligingsplan opgesteld onder leiding van de CISO en FG, gebaseerd op:
  - Dit IB&P beleid;
  - De uitkomsten van de jaarlijkse Eenduidige Normatiek Single Information Audit (ENSIA);
  - Andere audit resultaten;
  - Uitkomsten risico-analyses en DPIA's
  - Het dreigingsbeeld gemeenten van de IBD;
  - De door de teamleiders ingebrachte onderwerpen voor de informatievoorziening waarvoor zij verantwoordelijk zijn, bijvoorbeeld als uitkomst van een risicoanalyse of een privacy analyse (DPIA).

- Om uitvoering te kunnen geven aan dit strategisch beleid en het IB&P plan worden voldoende financiële middelen en uitvoeringscapaciteit ter beschikking gesteld.

2.7 Controle en verantwoording

Dit strategisch IB&P beleid is een verantwoordelijkheid van het bestuur van de gemeente Lelystad. De bestuurders en directeuren van de gemeente Lelystad zullen volgens de 10 principes voor informatiebeveiliging richting en sturing geven aan het onderwerp informatiebeveiliging en privacy door het geven van voorbeeldgedrag en het vragen om informatie.
Het directieteam is verantwoordelijk voor het gevraagd en ongevraagd rapporteren over informatiebeveiliging en privacy aan het College. Het directieteam rapporteert daarnaast over de mate waarin zij invulling hebben gegeven aan het uitwerken van tactische (deel) beleidsonderwerpen die aanvullend zijn op dit strategische beleid.

2.7.1 ENSIA

De gemeente verantwoordt zich over informatiebeveiliging middels de ENSIA-systematiek. Bij de gemeente Lelystad treedt de CISO op als ENSIA-coördinator. Deze zorgt ervoor dat de informatie die nodig is voor het beantwoorden van vragen binnen ENSIA wordt opgehaald bij de verantwoordelijke teamleiders. De teamleiders leveren alle informatie die nodig is voor het invullen van de jaarlijkse ENSIA-vragenlijsten.

De verantwoording over de informatiebeveiliging en privacybescherming komt in het jaarverslag tot uitdrukking in de collegeverklaringen Informatiebeveiliging en privacy. Met deze verklaringen geeft het college van B en W aan in hoeverre de gemeente voldoet aan de afspraken die gemaakt zijn voor de ENSIA-verantwoording Informatiebeveiliging en wettelijke eisen zoals uit de AVG. Ook worden de eventuele verbetermaatregelen vermeld die de gemeente gaat treffen. De ingevulde zelfevaluatievragenlijst vormt de basis voor het opstellen van de collegeverklaring aan de raad.

Met de ENSIA verantwoordt de gemeente zich ook aan de toezichthouders voor DIGID, BAG, BGT, BRO, Reisdocumenten, BRP, SUWI. Met de komst van de Cyberbeveiligingswet zal ook verantwoording worden afgelegd over informatiebeveiliging (BIO) aan de toezichthouder.

Middels deze verantwoording worden het bestuur van de gemeente Lelystad, de raad en landelijke toezichthouders geïnformeerd. De betrokkenheid van het bestuur is essentieel, en laat zien dat de gemeente Lelystad informatiebeveiliging serieus neemt en het een onderdeel laat zijn van de ambities om informatie van haar inwoners adequaat te beschermen.

Dit strategische beleid is op 15 april 2025 door het college van gemeente Lelystad vastgesteld

De interim secretaris
A.N. van den Bergh

de burgemeester,
A.E.H. Baltus

De vaststelling kan ook door middel van ondertekening van een collegebesluit-oplegger waarmee dit beleid behandeld wordt in de collegevergadering van de gemeente, in dat geval is deze ondertekening niet nodig.

Bijlage A: Privacyreglement Gemeente Lelystad

In dit reglement laat gemeente Lelystad zien op welke manier zij dagelijks omgaat met persoonsgegevens en privacy. Privacy speelt een belangrijke rol in de relatie tussen de burger en de overheid en staat daarmee hoog op de bestuurlijke agenda. Gemeenten hebben de verantwoordelijkheid over persoonsgegevens en gegevensuitwisseling op alle terreinen waar ze actief zijn. Gemeenten zijn verplicht om zorgvuldig en veilig, proportioneel en vertrouwelijk om te gaan met het verzamelen, bewaren en beheren van persoonsgegevens van burgers. Dat geldt voor taken op het gebied van basisadministraties, openbare orde en veiligheid, en het sociaal domein. Goed en zorgvuldig omgaan met persoonsgegevens is een dagelijkse bezigheid van gemeenten. Het beschermen van de privacy is complex, en wordt steeds complexer door technologische ontwikkelingen, de decentralisaties, grote uitdagingen op het terrein van veiligheid en nieuwe Europese wetgeving. Daarom vinden wij het belangrijk om transparant te zijn over de manier waarop wij met persoonsgegevens omgaan.

Artikel 1. Wetgeving en definities
Sinds 25 mei 2018 is de Algemene Verordening Gegevensbescherming (AVG), in Werking getreden, samen met de uitvoeringswet. De AVG zorgt onder andere voor versterking en uitbreiding van de privacyrechten met meer verantwoordelijkheden voor organisaties.

De volgende begrippen worden in de AVG gebruikt (Artikel 4, AVG):

Betrokkene: De persoon op wie de persoonsgegevens betrekking hebben. De betrokkene is degene van wie de gegevens worden verwerkt.

Verwerker: De persoon of organisatie die de persoonsgegevens verwerkt in opdracht van een andere persoon of organisatie.

Persoonsgegevens: Alle gegevens die gaan over mensen en waaraan je een mens als individu kunt herkennen. Het gaat hierbij niet alleen om vertrouwelijke gegevens, zoals over iemands gezondheid, maar om ieder gegeven dat te herleiden is tot een bepaald persoon (bijvoorbeeld; naam, adres, geboortedatum). Naast gewone persoonsgegevens kent de wet ook bijzondere persoonsgegevens. Dit zijn gegevens die gaan over gevoelige onderwerpen, zoals etnische achtergrond, politieke voorkeuren of het Burgerservicenummer (BSN).

Gegevensbeschermingseffectbeoordeling: Met een gegevensbeschermingseffectbeoordeling worden de effecten en risico's van de nieuwe of bestaande verwerkingen beoordeeld op de bescherming van de privacy. Dit heet ook wel een Privacy Impact Assessment (PIA).

Verwerkingsverantwoordelijke: Een persoon of instantie die alleen, of samen met een ander, het doel en de middelen voor de verwerking van persoonsgegevens vaststelt.

Verwerking: Een verwerking is alles wat je met een persoonsgegeven doet, zoals: vastleggen, bewaren, verzamelen, bij elkaar voegen, verstrekken aan een ander, en vernietigen.

Artikel 2. Reikwijdte
Het reglement is van toepassing op alle verwerkingen van persoonsgegevens door alle bestuursorganen van de gemeente. Oftewel: voor alle verwerkingen die binnen de gemeente plaatsvinden.

Artikel 3. Verantwoordelijke
De bestuursorganen van de gemeente zijn allemaal verantwoordelijken voor de verwerkingen die door of namens de gemeente worden uitgevoerd. De bestuursorganen van de gemeente zijn onder andere de burgemeester, het college van Burgemeesters en Wethouders (college van B&W) en de Raad.

Artikel 4. Verwerkingen (Artikel 4, AVG)
De verwerking van persoonsgegevens is elke handeling of elk geheel van handelingen met persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde processen. In de AVG valt onder een verwerking:
- Verzamelen, vastleggen en ordenen
- Bewaren, bijwerken en wijzigen
- Opvragen, raadplegen, gebruiken
- Verstrekken door middel van doorzending
- Verspreiding of enige andere vorm van ter beschikkingstellen
- Samenbrengen, met elkaar in verband brengen
- Afschermen, uitwissen of vernietigen van gegevens

Uit deze opsomming blijkt dat alles wat je met een persoonsgegeven doet een verwerking is.

Doeleinden (Artikel 5, AVG)
Volgens de wet mogen persoonsgegevens alleen verzameld worden als daarvoor een doel is vastgesteld. Het doel moet uitdrukkelijk omschreven en gerechtvaardigd zijn. De gegevens mogen niet voor andere doelen verwerkt worden. Voor de uitvoering van sommige wetten, zoals bijvoorbeeld de Jeugdwet, zijn de doelen voor het verwerken in de wet al vastgelegd, net als de persoonsgegevens die gevraagd en verwerkt mogen worden.

Rechtmatige grondslag (Artikel 6, AVG)
De wet zegt dat er voor elke verwerking van persoonsgegevens een rechtmatige grondslag uit de wet van toepassing moet zijn. Dat betekent dat de verwerking alleen mag plaatsvinden:
- Om een verplichting na te komen die in de wet staat
- Voor de uitvoering van een overeenkomst waar de betrokkene onderdeel was
- Om een ernstige bedreiging voor de gezondheid van de betrokkene te bestrijden
- Voor de goede vervulling van de gemeentelijke taak
- Wanneer de betrokkene toestemming heeft gegeven voor de specifieke verwerking

Wijze van verwerking
De hoofdregel van de verwerking van persoonsgegevens is dat het alleen toegestaan is in overeenstemming met de wet, en op een zorgvuldige wijze. Persoonsgegevens worden zoveel mogelijk verzameld bij de betrokkene zelf. De wet gaat uit van subsidiariteit. Dit betekent dat verwerking alleen is toegestaan wanneer het doel niet op een andere manier kan worden bereikt.
In de wet wordt ook gesproken over proportionaliteit. Dit betekent dat persoonsgegevens alleen mogen worden verwerkt als dit in verhouding staat tot het doel. Wanneer met geen, of minder (belastende), persoonsgegevens hetzelfde doel bereikt kan worden moet daar altijd voor gekozen worden.
De gemeente zorgt ervoor dat de persoonsgegevens kloppen en volledig zijn voordat ze verwerkt worden. Deze gegevens worden alleen verwerkt door personen met een geheimhoudingsplicht. Daarnaast beveiligt de gemeente alle persoonsgegevens. Dit moet voorkomen dat de persoonsgegevens kunnen worden ingezien of gewijzigd door iemand die daar geen recht toe heeft.
Hoe de gemeente dit doet staat in dit informatiebeveiligingsbeleid van de gemeente en in een eventueel aanvullend beveiligingsplan specifiek opgesteld voor een proces of registratie.

Doorgifte (Artikel 44 t/m 50, AVG)
De gemeente geeft in beginsel geen persoonsgegevens door met een land buiten de Europese Economische Ruimte (EER) of een internationale organisatie.

Artikel 5. Transparantie en communicatie
Wet open overheid (Woo)
Via de Wet Open Overheid kun je een verzoek om informatie indienen bij de gemeente. Bij het verzoek bekijkt de gemeente altijd of het antwoord geen inbreuk maakt op de persoonlijke levenssfeer van betrokkenen. In principe worden geen persoonsgegevens verstrekt.

Wet hergebruik van overheidsinformatie
De Wet hergebruik van overheidsinformatie regelt het op verzoek verstrekken van overheidsinformatie voor hergebruik. Bij het verzoek bekijkt de gemeente altijd of het antwoord geen inbreuk maakt op de persoonlijke levenssfeer van betrokkenen. In principe worden geen persoonsgegevens verstrekt.

Informatieplicht (Artikel 13,14, AVG)
De gemeente informeert betrokkenen over het verwerken van persoonsgegevens. Wanneer betrokkenen gegevens aan de gemeente geven, worden zij op de hoogte gesteld van de manier waarop de gemeente met persoonsgegevens om zal gaan. Dit kan bijvoorbeeld via een formulier gebeuren. De betrokkene wordt niet nogmaals geïnformeerd als hij/zij al weet dat de gemeente persoonsgegevens van hem/haar verzamelt en verwerkt, en weet waarom en voor welk doel dat gebeurt. Wanneer de gegevens via een andere weg verkregen worden, dus buiten de betrokkene om, wordt de betrokkene geïnformeerd op het moment dat deze voor de eerste keer worden verwerkt.

Verwijdering
De gemeente bewaart de persoonsgegevens niet langer dan nodig is voor de uitvoering van gemeentelijke taken, of zoals vastgelegd in de Archiefwet. Wanneer er nog persoonsgegevens opgeslagen zijn die niet langer nodig zijn voor het bereiken van het doel worden deze zo snel mogelijk verwijderd. Dit houdt in dat deze gegevens vernietigd worden, of zo worden aangepast dat de informatie niet meer gebruikt kan worden om iemand te identificeren. Teams stellen zich op de hoogte van de eventuele bewaartermijn en bewaken de bewaartermijn.

Rechten van betrokkenen (Artikel 13 t/m 20, AVG)

De wet bepaalt niet alleen de plichten van degenen die de persoonsgegevens verwerken, maar bepaalt ook de rechten van de personen van wie de gegevens worden verwerkt. Deze rechten worden ook wel de rechten van betrokkenen genoemd, en bestaan uit de volgende rechten:

- Recht op informatie: Betrokkenen hebben het recht om aan de gemeente te vragen of zijn/haar persoonsgegevens worden verwerkt.
- Inzagerecht: Betrokkenen hebben de mogelijkheid om te controleren of, en op welke manier, zijn/haar gegevens worden verwerkt.
- Correctierecht: Als duidelijk wordt dat de gegevens niet kloppen, kan de betrokkene een verzoek indienen bij de gemeente om dit te corrigeren.
- Recht van verzet: Betrokkenen hebben het recht aan de gemeente te vragen om hun persoonsgegevens niet meer te gebruiken.
- Recht om vergeten te worden: In gevallen waar de betrokkene toestemming heeft gegeven om gegevens te verwerken, heeft de betrokkene het recht om de persoonsgegevens te laten verwijderen.
- Recht op bezwaar: Betrokkenen hebben het recht om bezwaar aan te maken tegen de verwerking van zijn/haar persoonsgegevens. De gemeente zal hieraan voldoen, tenzij er gerechtvaardigde gronden zijn voor de verwerking.

Indienen van verzoek
Om gebruik te maken van zijn/haar rechten kan de betrokkene een verzoek indienen. Dit verzoek kan zowel schriftelijk als via de e-mail ingediend worden (fg@lelystad.nl). De gemeente heeft vier weken de tijd, vanaf de ontvangst van het verzoek, om te beoordelen of het verzoek gerechtvaardigd is. Deze termijn kan eenmalig met 2 maanden worden verlengd. Binnen vier weken zal de gemeente laten weten wat er met het verzoek gaat gebeuren. Als het verzoek niet wordt opgevolgd is er de mogelijkheid om bezwaar te maken bij de gemeente, of een klacht in te dienen bij de Autoriteit Persoonsgegevens (AP). Aan de hand van een verzoek kan de gemeente aanvullende informatie opvragen om zeker te zijn van de identiteit van de betrokkene.

Artikel 6. Geautomatiseerde verwerkingen
Datateam
Het datateam verzamelt, verwerkt en analyseert gegevens om organisaties te helpen bij het nemen van data-gedreven beslissingen.
Het datateam is lid van de Vereniging voor Statistiek en Onderzoek. Daarmee hebben ze zich gecommitteerd aan werken volgens de standaarden in de gedragscode voor statistisch onderzoek. Deze gedragscode waarin de AVG ruimschoots aan bod komt, is hier te vinden: Gedragscode voor Statistisch Onderzoek | De Vereniging voor Beleidsonderzoek
Bij een datavraag vanuit de organisatie wordt de privacy flowchart gebruikt. En zonodig het project startdocument dat onder meer antwoord geeft op de vraag welke grondslag wordt gebruikt voor het verwerken van gegevens.

Inzet van camera's
Binnen de gemeente wordt onder bepaalde omstandigheden gebruik gemaakt van cameratoezicht, zoals vastgelegd in de Gemeentewet. Cameratoezicht wordt onder andere gebruikt voor het vergroten van de veiligheid op straat. Camera's kunnen een grote inbreuk maken op de privacy van diegene die gefilmd worden. Om de privacy zo goed mogelijk te waarborgen worden camera's alleen ingezet wanneer er geen andere manieren zijn om het doel te bereiken, en worden er eisen gesteld aan de inzet van camera's.
Gemeente Lelystad maakt gebruik van cameratoezicht en houdt zich daarbij aan het vastgestelde camera-reglement.

Artikel 7. Plichten van de gemeente
Register van verwerkingen (Artikel 30, AVG)
De gemeente is verantwoordelijk voor het aanleggen van een register van alle verwerkingen waarvan de gemeente de verwerkingsverantwoordelijke is. Elk register bevat een beschrijving van wat er tijdens een verwerking plaatsvindt, en welke gegevens daarvoor worden gebruikt, namelijk:

- De naam en contactgegevens van de verwerkingsverantwoordelijke en, mogelijk, de gezamenlijke verwerkingsverantwoordelijke;
- De inhoud en doelen van de verwerking;
- Een beschrijving van het soort persoonsgegevens en de daarbij horende betrokkenen;
- Een beschrijving van de ontvangers van de persoonsgegevens;
- De termijnen waarin de verschillende persoonsgegevens moeten worden gewist;

Gegevensbeschermingseffectbeoordeling (Artikel 35, AVG)
Met een gegevensbeschermingseffectbeoordeling worden de effecten en risico's van nieuwe of bestaande verwerkingen beoordeeld op de bescherming van de privacy. De gemeente voert deze uit wanneer er een geautomatiseerde verwerking, een grootschalige verwerking, of wanneer er een grootschalige

monitoring van openbare ruimten plaatsvindt. Dit geldt in het bijzonder bij verwerkingen waarbij nieuwe technologieën worden gebruikt.

Artikel 8. Verwerker
Indien de verantwoordelijke persoonsgegevens laat verwerken door een bewerker vindt verwerking uitsluitend plaats indien voorafgaand aan die verwerking een daartoe strekkende overeenkomst tussen de verantwoordelijke en de bewerker is gesloten. Er wordt bij voorkeur gebruik gemaakt van de standaard verwerkersovereenkomst van de gemeente Lelystad. De FG (functionaris gegevensbescherming) houdt een register bij van verwerkersovereenkomsten. De verantwoordelijke meldt een nieuwe verwerkers-overeenkomst bij de FG

Artikel 9 Datalekken (Artikel 33,34, AVG)
We spreken van een datalek wanneer persoonsgegevens in handen vallen van derden die geen toegang tot die gegevens mogen hebben. Datalekken worden meten aan de FG gemeld. Wanneer er een ernstig datalek heeft plaatsgevonden meldt de FG dit zonder onredelijke vertraging, uiterlijk 72 uur nadat er kennis van de inbreuk is vernomen, aan de Autoriteit Persoonsgegevens. Als dit later dan 72 uur is wordt er een motivering voor de vertraging bij de melding gevoegd. Het kan zijn dat de inbreuk een hoog risico met zich meebrengt voor de rechten en vrijheden van de betrokkenen. In dit geval meldt de gemeente (te weten het betreffende team waar het datalek heeft plaatsgevonden) dit aan de betrokkenen in eenvoudige en duidelijke taal. Om toekomstige datalekken te voorkomen worden bestaande datalekken geëvalueerd. De FG coördineert de afhandeling van datalekken.

Aanstellen van een Functionaris voor gegevensbescherming (FG) (Artikel 37 t/m 39, AVG)
De gemeente heeft een FG aangesteld. De FG is betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens. De taken van de functionaris zijn informeren, adviseren, toezicht houden, bewustwording creëren, en optreden als contactpersoon van het AP.
Het is niet de bedoeling dat de functionaris de taken op het gebied van bescherming van de privacy van de afdelingen overneemt. De afdelingen hebben hun eigen verantwoordelijkheid in het goed omgaan met privacygevoelige gegevens. Een verwerking van persoonsgegevens wordt eerst aan de FG gemeld voordat de verwerking begint. De FG is verantwoordelijk voor het structureel toetsen van de implementatie en de uitvoering van de wettelijke eisen en de gemeentelijke richtlijnen op het gebied van privacy. De FG op het gebied van de AVG is dat tevens voor de Wpg.
Voor vragen over privacy of over deze toelichting kunt u contact opnemen met de functionaris voor gegevensbescherming van gemeente Lelystad via: fg@lelystad.nl

Taken en bevoegdheden functionaris gegevensbescherming (Artikel 37 t/m 39, AVG)
Artikel 10. Taken FG
1. Binnen de gemeente Lelystad is een FG aangesteld als bedoeld in artikel 37-39 van de AVG
2. De FG heeft naast het houden van toezicht als bedoeld in artikel 37-39 van de AVG in ieder geval tot taak:
    a. Het toezicht houden op wijzigingen in bestaande verwerkingen en het aanleggen van nieuwe verwerkingen met persoonsgegevens; een ieder binnen de organisatie, die persoonsgegevens verzamelt en verwerkt deelt, voordat met de verzameling en verwerking wordt begonnen, dit mee aan de FG voor zover het nog niet in het register is opgenomen.
    b. Het geven van advies over de toepassing van de AVG bij de gemeente Lelystad, met medewerking van de privacy officer;
    c. Het inrichten en onderhouden van het register als bedoeld in artikel 7 van dit besluit;
    d. Uitvoeren van audits op basis van een risico-analyse.
    e. Het jaarlijks opstellen van een verslag van zijn werkzaamheden. Dit verslag wordt gezonden aan de verantwoordelijke;

Artikel 11 Beveiliging, beheer en auditing
1. De FG toetst op basis van een jaarlijkse risico-analyse de technische en organisatorische maatregelen om de persoonsgegevens te beveiligen tegen verlies, diefstal en onrechtmatige verwerking en raadpleging. Het team is verantwoordelijk voor het doorvoeren van beheersmaatregelen. De FG toetst vanuit de auditrol de effectiviteit van deze beheersmaatregelen.
2. Indien de FG onrechtmatigheden aantreft bij de verwerking van persoonsgegevens brengt hij hierover verslag uit aan het hoofd van het betreffende team. Hij doet dit verslag vergezeld gaan van een aanbeveling, die strekt tot een verbetering van de bescherming van persoonsgegevens, die door of namens de verantwoordelijke worden verwerkt.
3. Indien de aanbeveling niet of niet voldoende wordt opgevolgd, rapporteert de FG zijn bevindingen aan de verantwoordelijke.

Artikel 12 Toegang verlenen

1. De FG is bevoegd elke plaats in de gebouwen op de terreinen die bij de gemeente in gebruik zijn en waar persoonsgegevens worden verwerkt te betreden;
   De FG is bevoegd inlichtingen te vorderen van een ieder die onder gezag van het college van burgemeester en wethouders of de burgemeester werkzaam is.

Artikel 13 Bevoegdheid tot inzage
1. De FG is bevoegd inzage te vorderen van zakelijke gegevens en bescheiden waarin persoonsgegevens zijn verwerkt.
2. Hij is bevoegd van de gegevens en bescheiden kopieën te maken.
3. Indien het maken van kopieën niet ter plekke kan gebeuren, is hij bevoegd de gegevens en bescheiden voor maximaal één dag mee te nemen.

Artikel 14 Weigering
1. Indien de medewerking voor het verstrekken van inlichtingen als bedoeld in artikel 12 en het verzoek tot inzage als bedoeld in artikel 13 wordt geweigerd, kan het college van burgemeester en wethouders, op een met redenen omkleed verzoek van de FG, toestemming verlenen zelfstandig de nodige inlichtingen te verzamelen dan wel de persoonsgegevens in te zien;
2. Het college van burgemeester en wethouders wordt zo spoedig mogelijk in kennis gesteld van de uitkomsten van dit onderzoek, waarbij ook het directieteam wordt ingelicht.

Artikel 15 Geheimhouding
De FG is verplicht tot geheimhouding van hetgeen hem op grond van een klacht of een verzoek van betrokkene is bekend geworden, tenzij betrokkene in bekendmaking toestemt.

Artikel 16 Ingangsdatum regeling
Deze regeling treedt in werking met ingang van 25 maart 2025.

Afsluiting
Als de gemeente een wettelijke verplichting niet nakomt kan de betrokkene een klacht indienen. Deze zal via de klachtenregeling van de gemeente worden behandeld. In gevallen waar het reglement niets over zegt, beslist het verantwoordelijke bestuursorgaan van de gemeente.
Dit privacyreglement gebaseerd op de AVG vervangt het privacyreglement van 25 mei 2018.
Op de website **https://www.gemeentelelystad.nl/privacy** is het Privacy Statement opgenomen.

Disclaimer:
Dit product is een eenvoudige en begrijpbare vertaling van de huidige privacywetgeving en gebaseerd op de AVG. Vanzelfsprekend is de toepasbare wet- en regelgeving altijd leidend en kunnen er geen rechten ontleend worden aan dit document. Op de website **https://www.gemeentelelystad.nl/privacy** *is een Privacy Statement opgenomen*

Bijlage B: Organisatie, taken & verantwoordelijkheden

Deze bijlage geeft op hoofdlijnen inzicht in de ambtelijke rollen en is ter informatie bijgevoegd aan dit strategisch beleid.

Gemeentesecretaris
Ambtelijk is de gemeentesecretaris eindverantwoordelijk voor de integrale beveiliging en voor de inrichting en werking van de IB&P-organisatie en Bedrijfscontinuïteitsmanagement (BCM). In die hoedanigheid is hij eindverantwoordelijk voor de implementatie van alle beveiligings- en privacykaders in zijn organisatie. En laat zich daarbij adviseren door functionarissen, zoals een Chief Information Security Officer (CISO), Chief Information Officer (CIO) en Functionaris Gegevensbescherming (FG).

Directieteam
Het directieteam:

- Zorgt dat alle (persoons)gegevens, processen en systemen en de daarbij behorende middelen altijd onder de verantwoordelijkheid vallen van een teamleider.
- Zorgt dat de teamleiders zich verantwoorden over de beveiliging en de privacy van de (persoons)gegevens of andere informatie die onder hen berust.
- Zorgt dat de teamleiders toezien op de *beschikbaarheid*, *integriteit* en *vertrouwelijkheid* van informatie in hun proces; en dat zij voorbereid zijn op een calamiteit (Bedrijfscontinuïteit).
- Zorgt dat het college gevraagd en ongevraagd geïnformeerd wordt over de mate waarin informatiebeveiliging een onderdeel is van het handelen van de bedrijfsvoering. Op die manier kan het college zich ook verantwoorden naar de raad.
- Stelt het gewenste niveau van continuïteit en vertrouwelijkheid vast.
- Draagt zorg voor het uitwerken van tactische informatiebeveiligings- en privacybeleidsonderwerpen en laat zich hierin bijstaan door de CISO en FG van de gemeente.
- Autoriseert de benodigde procedures en uitvoeringsmaatregelen.
- Ziet het onderwerp informatiebeveiliging en privacybescherming binnen de gemeente Lelystad als een integraal onderdeel van risicomanagement.

Teamleiders
De uitvoering van informatiebeveiliging en privacybescherming valt onder de verantwoordelijkheden van alle teamleiders[7]. Teamleiders zijn verantwoordelijk voor het behoud van de vertrouwelijkheid, integriteit (juistheid & volledigheid) en beschikbaarheid van informatie in de hele keten van hun proces; dus inclusief ketenpartners, leveranciers, (cloud)systemen, Internet of Things (IoT), Operationele Technologie (OT). Om deze verantwoordelijkheid waar te maken dienen zij goed ondersteund te worden vanuit de tweede lijn (PO, ISO, applicatie- en systeembeheerder). Deze verantwoordelijkheid kunnen zij niet delegeren, uitvoerende werkzaamheden wel.

7) In de BIO wordt een teamleider aangeduid als proceseigenaar.