GEMEENTEBLAD
Officiële uitgave van de gemeente Westland
Nr. 163405
15 april
2024

Gegevensbeschermingsbeleid 2024-2026

De raad van de gemeente Westland;

gelezen het voorstel van burgemeester en wethouders van 13 februari 2024, met de volgende bijlage(n):

- Gegevensbeschermingsbeleid 2024-2026

gelet op het bepaalde in artikel 24 lid 2 Algemene Verordening Gegevensbescherming en

gelet op het bepaalde in verplichte maatregel 5.1.2.1. Baseline Informatiebeveiliging Overheid;

gehoord het advies van de commissie Bestuur en Economie van 14 maart 2024 en gehoord de beraadslagingen van onderhavige vergadering;

besluit:

1. Het gegevensbeschermingsbeleid 2024-2026 vast te stellen.

1. Inleiding

In 2020 is het eerste gegevensbeschermingsbeleid geschreven. Dit lijkt nog maar kort geleden. Maar de wereld van informatiebeveiliging en privacy staat niet stil. Naast een veranderende wereld met nieuwe technologieën en geopolitieke verschuivingen, hebben wij ook te maken met nieuwe wetgeving die zich specifiek richt op de bescherming van informatie.
Daarom schrijven wij nu dit nieuwe gegevensbeschermingsbeleid. Hierin beschrijven wij hoe gemeente Westland omgaat met informatie en persoonsgegevens. Hiermee willen wij uitdragen dat burgers en bedrijven, maar ook de medewerkers er op kunnen vertrouwen dat gemeente Westland zorgvuldig omgaat met alle informatie en persoonsgegevens die binnen de organisatie verwerkt worden.
Dit nieuwe beleid schrijven wij met een frisse blik op de toekomst. We beschrijven de pijlers waar wij onze activiteiten aan koppelen. Zodat wij compliant zijn aan wetgeving, oog hebben voor risico's binnen en buiten de organisatie en met elkaar kritisch bezien of alles wat met data mogelijk is, ook al-tijd wenselijk is.
We brengen in beeld wie welke taken in de organisatie heeft. En koppelen deze aan de bestuurlijke principes van de Informatiebeveiligingsdienst (IBD). We werpen een blik op nieuwe wet- en regelgeving. Tot slot beschrijven we welke stappen wij moeten ondernemen om hieraan te voldoen.

1.1 Informatiebeveiliging

Onder informatiebeveiliging verstaan we:

'het treffen en onderhouden van een samenhangend pakket van maatregelen om de betrouw-baarheid van de informatievoorziening aantoonbaar te waarborgen'.

Kernpunten daarbij zijn:
- beschikbaarheid,
- integriteit (juistheid) en
- vertrouwelijkheid.

Dit geldt voor (persoons)gegevens en andere informatie.
Het gegevensbeschermingsbeleid 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. Het heeft betrekking op het politieke bestuur, alle medewerkers, burgers, gasten, bezoekers en ex-terne relaties.

1.2 Privacy (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 van burgerzaken. Om als gemeente deze taken goed uit te voeren zijn persoonsgegevens noodzakelijk.

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.

2. Managementsamenvatting

In navolging van het Gegevensbeschermingsbeleid 2020-2023 is er een gegevensbeschermingsbe-leid 2024-2026 opgesteld.
Dit beleid is in lijn met de toekomstvisie van het team Gegevensbescherming (onderdeel van Juridische zaken, Inkoop en Gegevensbescherming). In de toekomstvisie worden drie pijlers benoemd:

- Compliant

De organisatie moet compliant zijn (voldoen) aan de relevante wet- en regelgeving.

- Preventief

We moeten voorbereid blijven en anticiperen op risico's vanuit de buitenwereld

- Ethiek

De gemeente moet bij uitvoering van alle processen het belang en de rechten en vrijheden van de betrokkenen niet uit het oog verliezen.

Het samenspel tussen deze drie pijlers zorgen voor een optimaal beschermde organisatie. Dat is onze stip aan de horizon,

Dreigingen
Externe risico's door o.a. cybercriminelen en statelijke actoren zorgen ervoor dat we doorlopend alert moeten zijn, om de informatie en persoonsgegevens van inwoners afdoende te beschermen. Alles tegelijk beveiligen is onmogelijk. Daarom doen we dit risicogestuurd, waarbij de grootste risico's de hoogste prioriteit krijgen.

Wij houden vast aan de 10 principes voor gegevensbescherming. Op basis van de principes van de IBD, onderdeel VNG.
De principes zijn;

- Bestuurders bevorderen een veilige cultuur.
- Gegevensbescherming is van iedereen.
- Gegevensbescherming is risicomanagement.
- Risicomanagement is onderdeel van de besluitvorming.
- Gegevensbescherming behoeft ook de aandacht in (keten)samenwerking.
- Gegevensbescherming is een proces.
- Gegevensbescherming kost geld.
- Onzekerheden dient te worden ingecalculeerd.
- Verbetering komt voort uit leren en ervaring.
- Het bestuur controleert en evalueert.

De gemeente werkt veel samen met andere partijen daarom is het een speerpunt om ook in de keten afspraken te maken over informatiebeveiliging en privacy,

Voortdurende verbetering is noodzakelijk en daarom volgen wij het principe van Plan-Do-check-Act. Het doorlopen van de cyclus wordt geregistreerd in het Information Security Management System (ISMS) en het Privacy Management System (PMS). Rollen en verantwoordelijkheden worden vastgelegd door middel van het RASCI-model.

De voortdurende verbeteringen willen wij in 2026 extern laten toetsen, waarbij het doel is een ISO27001 (informatiebeveiliging) en een privacy certificering te behalen.

3. Visie

Eind 2022 maakten wij een start met de toekomstvisie op gegevensbescherming voor de organisa-tie. Al onze doelen hangen wij op aan een drietal pijlers:

- compliant;
- preventief;

- ethiek.

Wij kozen voor deze drie pijlers, omdat ze samen een geheel vormen. Als aan deze drie pijlers vol-daan wordt, ontstaat een zo veilig mogelijke organisatie. Waarin wij in control zijn en waarbij de rechten van de burger ook beschermd worden.
Er staat een zo veilig mogelijke organisatie, omdat 100% veilig niet bestaat.

3.1 Compliant
De organisatie moet compliant zijn (voldoen) aan de relevante wet- en regelgeving. Dit zijn onder andere de Algemene Verordening Gegevensbescherming (AVG) en de Baseline Informatiebeveili-ging Overheid (BIO) en de Archiefwet. Maar de organisatie wordt daarnaast ook getoetst op de eisen m.b.t. gegevensbescherming in specifieke wetgeving, zoals de Wet Politiegegevens (WPG), Wet Ba-sisregistratie Personen (Wet BRP), Wet digitale overheid (WDO) en Wet SUWI.

3.2 Preventief
We moeten alert zijn op de risico's vanuit de buitenwereld. En hierop voorbereid blijven en anticiperen. Cybercriminaliteit is een verdienmodel geworden. De organisatie heeft een schat aan informa-tie. Deze is voor velen interessant. Het is de taak van de hele organisatie en iedere medewerker om al deze gegevens goed te beschermen.

3.3 Ethiek
De gemeente moet bij uitvoering van alle processen het belang en de rechten en vrijheden van de betrokkenen niet uit het oog verliezen. Bij beleidskeuzes en gebruik van business intelligence is een bewuste belangenafweging noodzakelijk. Hierbij is het belang van de inwoners of aanvragers onze prioriteit.

We zijn transparant over wat er met de gegevens van de inwoners en bedrijven gebeurt door regis-ters openbaar te maken. In het verwerkingsregister staan de processen en welke persoonsgegevens gebruikt worden. In het algoritmeregister worden het gebruik van impactvolle inzet van algoritmes en in welke systemen dit plaatsvindt.

3.4 Samenspel 3 pijlers
100% compliance aan de BIO en de AVG zorgen niet voor een optimaal veilige organisatie. Cyber-criminelen verzinnen altijd nieuwe manieren om binnen te komen. Daarnaast is het mensenwerk. Mensen kunnen altijd een fout maken. Door op een verdachte link te klikken of een brief met per-soonsgegevens naar een verkeerd adres te sturen. Compliance staat dus niet gelijk aan veilig.

Om de cybercriminelen voor te zijn, nemen we preventieve maatregelen. Dit zijn vaak actuele maatregelen, die genomen worden op basis van een advies van een leverancier of de IBD. Vaak naar aanleiding van nieuwe kwetsbaarheden. Daarnaast trainen we onze medewerkers. Dit gebeurt in nauw overleg met de mensen van de Westland Academie. Zij faciliteren de leerlijn "Werken in West-land". De medewerkers moeten jaarlijks een aantal verplichte trainingen volgen. Dus compliance aan wet- en regelgeving en het nemen van preventieve maatregelen zorgen voor bescherming tegen (ac-tuele) dreigingen.
De eerste twee pijlers zijn vooral gericht op dreigingen van buitenaf. Maar ethiek richt zich meer op de organisatie zelf. Er zijn steeds meer technologische mogelijkheden om informatie te gebruiken en informatiebronnen met elkaar te verbinden. En hier bijvoorbeeld patronen in te ontdekken. De vraag is of we dit in alle gevallen wel moeten willen. Kan deze nieuwe informatie misschien stigmatiserend werken? Of is het geconstateerde patroon wel een echt patroon of een persoonlijke interpretatie van de informatie? Om te voorkomen dat hier vervelende situaties voor burgers ontstaan, willen wij dat de organisatie ethische aspecten meeneemt in de processen en bij het gebruik van informatie.

Zo zorgen deze drie pijlers dat er naar wet- en regelgeving gekeken wordt. Met een scherpe blik naar buiten, maar ook een kritische blik naar binnen. En zonder de actualiteit uit het oog te verliezen. Zo komen we met elkaar in control op informatiebeveiliging en privacy.

3.5 Stip op de horizon
In 2026 aantoonbaar in control zijn. Dat is onze stip op de horizon. Hiervoor is een toekomstvisie gegevensbescherming opgesteld en maken wij strategische plannen. Wij stellen ons als doel om in 2026 zowel op informatiebeveiliging als privacy een certificering te behalen. Voor informatiebeveili-ging is dit de ISO 27001 en voor de privacy op basis van de AVG.
Zo willen wij de Westlandse burgers en ondernemingen kunnen tonen dat gemeente Westland haar zaken goed op orde heeft. Dat geeft vertrouwen en zou helemaal GOUD zijn!

Omdat de wereld niet stil staat, nemen we preventieve maatregelen om de risico's voor onze organisatie, inwoners en ondernemers tot een aanvaardbaar niveau terug te brengen

4. Risico en dreiging

De externe dreigingen nemen de laatste jaren steeds meer toe. Naast de cybercriminelen die vanuit winstbejag pogingen doen om een organisatie te besmetten met gijzelsoftware of door middel van CEO-fraude een bedrag overgemaakt proberen te krijgen, gebeurt er ook veel op internationaal ni-veau. De veranderingen in de geopolitieke situatie maakt dat het risico op een digitale aanval op een onderdeel van de Nederlandse overheid steeds groter wordt. Het Nationaal Cyber Security Center (NCSC) brengt elk kwartaal rapportages uit over deze dreigingen.

Statelijke actoren
Tot nu toe zijn de risico's niet specifiek op Nederlandse gemeenten gericht. Maar dat betekent niet dat gemeenten niet het slachtoffer kunnen worden. Vaak wordt er bij wijze van spreken met een schot hagel geschoten. De kans dat dan iets geraakt wordt, is altijd aanwezig. Hierbij valt te denken aan DDoS aanvallen, waarbij een website dusdanig zwaar belast wordt, dat deze op 'zwart' gaat.

We zien ook een toename van digitale spionage door landen met een offensief cyberprogramma tegen Nederland. Hierbij wordt specifiek aandacht gevraagd voor mobiele telefoons, waar ongemerkt spionagesoftware op geïnstalleerd wordt.
Door alle aanwezige sensoren op een smartphone verzamelen deze apparaten veel informatie over de gebruiker. Statelijke actoren kunnen deze informatie gebruiken om personen van belang te identi-ficeren, profileren en lokaliseren.

Hacktivisten
Bovenstaande dreiging kan ontstaan door toedoen door een buitenlandse overheid, maar ook door hacktivisten, die zich verbonden hebben aan de doelen van landen met een offensief cyberpro-gramma tegen Nederland.

Terroristen
Terroristen staan los van landen, maar verbinden zich aan een bepaalde overtuiging. Zij kunnen ook getriggerd worden door gebeurtenissen in Nederland en Europa. Zoals bijvoorbeeld een cartoon of het verbranden van een Koran.

Wij beoordelen kritisch de risico's en nemen weloverwogen besluiten, waarbij de belangen van de burger centraal staan

4.1 Risico gestuurd
De organisatie loopt vele risico's. Om de bedrijfsvoering niet in gevaar te brengen, moeten we deze terugbrengen tot een acceptabel risico, het zogenaamde geaccepteerde risico. Dit is een risiconi-veau waar de organisatie zich op basis van de risicobereidheid prettig bij voelt. Het is aan elke orga-nisatie om het eigen geaccepteerde risico te bepalen. Dit geaccepteerde risico is gebaseerd op de grootte van de impact van de schade, de waarde van het product en de kosten om deze te voorko-men. Het is van belang om per proces goed te bepalen wat de risico's zijn en wat het geaccepteerde risico is.
Ditzelfde geldt bij een incident of kwetsbaarheid. Op risico gestuurde wijze wordt bepaald welke processen prioriteit hebben.
Op basis van een BIO-toets en een DPIA (Data Privacy Impact Assessment) voeren we analyses op processen uit. En bepalen we welke maatregelen genomen moeten worden om de bij dit proces behorende risico's naar een acceptabel niveau terug te brengen. Dit soort analyses worden bij voorkeur bij proceswijzigingen of implementatie van het proces uitgevoerd.

Voldoen aan toepasselijke kaders, normen, wetten en regelgeving is een randvoorwaarde voor alle gemeentelijke processen.

5. Randvoorwaarden

Gemeente Westland stelt het gegevensbeschermingsbeleid op vanuit een integrale benadering, informatiebeveiliging en privacy. Het gegevensbeschermingsbeleid is een strategisch beleid dat wordt vastgesteld door het college. Daar waar nodig wordt het tactisch beleid door de verantwoordelijke teams opgesteld.
Verder worden in onder meer de Digitale Agenda Gemeenten 2024 en Agenda Digitale Veiligheid 2020-2024 belangrijke ontwikkelingen voor gemeenten genoemd op het gebied van informatievoor-ziening, digitalisering en veiligheid. Dit is ook vastgelegd in de resolutie "Digitale Veiligheid: kern-taak voor gemeenten". Hierbij is betrokkenheid van het bestuur cruciaal. Dit is onder andere ver-woord in de tien bestuurlijke principes voor informatiebeveiliging van de VNG.

Dit betekent dat ook onze organisatie continu moet investeren. Niet alleen in technische beveili-gingsmaatregelen, maar juist ook in de mens (bewustwording, houding, gedrag), een veilige organi-satie, veilige gereedschappen en een open cultuur.

De 10 principes voor informatiebeveiliging zijn een bestuurlijke aanvulling op het normenkader BIO en gaan over de waarden die de bestuurder zichzelf oplegt.
De Gemeente Westland heeft bepaald dat deze principes ook van toepassing zijn voor privacy.
De principes worden dan als volgt;

- Bestuurders bevorderen een veilige cultuur.
- Gegevensbescherming is van iedereen.
- Gegevensbescherming is risicomanagement.
- Risicomanagement is onderdeel van de besluitvorming.
- Gegevensbescherming behoeft ook de aandacht in (keten)samenwerking.
- Gegevensbescherming is een proces.
- Gegevensbescherming kost geld.
- Onzekerheden dient te worden ingecalculeerd.
- Verbetering komt voort uit leren en ervaring.
- Het bestuur controleert en evalueert.

5.1 Scope van het Gegevensbeschermingsbeleid

Belangrijke Europese en landelijke wettelijke kaders voor privacy zijn de GDPR (AVG) en landelijk de BIO voor informatiebeveiliging maar ook de Archiefwet. Daarnaast kunnen de collegeprogramma's en gemeentelijke visies een kader vormen voor informatieveiligheid en privacy.
De scope van dit beleid omvat alle informatieprocessen en -systemen die de gemeente uitvoert en beheert ten behoeve van de gemeente en de partners die deze gebruiken. Het beleid heeft niet al-leen betrekking op de verwerking, uitwisseling en opslag van digitale informatie, maar ook op de informatie in fysieke of analoge vorm. Ongeacht de locatie, het tijdstip of de gebruikte apparatuur. Organisatorisch zijn de uitgangspunten uit dit beleid van toepassing op zowel de raad, het college als de ambtelijke organisatie. Alle strategische beleidsuitgangspunten met betrekking tot informatie-veiligheid en privacy, en de organisatie ervan zijn in dit organisatie brede document samenge-bracht.
Alle relevante wetgeving is opgenomen in de bijlage normenkader.

De Archiefwet stelt algemene eisen aan het beheer van alle archiefbescheiden van de overheid. (Daaronder valt o.a. het borgen van een goede, geordende en duurzame toegankelijkheid van infor-matie alsmede het verplicht bewaren c.q. vernietigen van informatie volgens de Selectielijst.)

De Wet Politiegegevens (WPG) geeft de gemeente privacykaders voor de taken van de BOA's die bij de gemeente in dienst zijn. Zij verwerken gegevens die niet onder de AVG vallen maar onder de WPG. Hiervoor stelt de gemeente beleid en samenhangende procedures op die betrekking hebben op toegangsrechten, autorisaties, data classificatie, risico-inschatting, registratie en logging, meld-plicht en documentatieplicht.

De Wet Digitale Overheid (WDO) is een nieuwe wet. Deze treedt gefaseerd in werking. De eerste tranche trad op 1 juli 2023 in werking en richt zich voornamelijk op digitale toegang, zoals DigiD en eIDAS. De wet geldt pas als een instantie technisch en organisatorisch klaar is om aan te sluiten. Hiervoor stellen de departementen, de publieke dienstverleners én Logius samen een aansluitsche-ma op.

De komst van de NIS2 (richtlijn voor netwerk- en informatiesystemen) betekent dat er op het gebied van wet- en regelgeving voor informatieveiligheid zaken gaan veranderen. De NIS2 moet nog in na-tionale wetgeving ondergebracht worden. Het is nog niet geheel duidelijk welke wet dit zal gaan worden. Dit kan in de WDO zijn, maar ook in een nieuwe versie van de Wet Beveiliging Netwerk en In-formatiesystemen (WBNI).
Dit alles is ook van invloed op de komst van de BIO 2.0. De BIO 2.0 is een nieuwe versie van de BIO die gebaseerd is op de laatste versie van de ISO 27001:2022. Op dit moment vinden er nog gesprek-ken plaats over de inhoud en de datum van publicatie van de BIO 2.0.

- Het programma eigentijdse ICT is begin 2023 gestart met als doel om de Westlandse ICT te moderniseren. Een groot deel van de systemen zal in de komende tijd gemigreerd worden naar het Microsoft Azure platform. Verder worden er aanvullende maatregelen genomen rondom back-up en redundancy. Na het afronden van het programma eigentijdse ICT is ge-meente Westland op het gebied van ICT BIO compliant.

Algoritmes/ Artificial intelligence

Naast de modernisering van de Westlandse ICT, zijn er ook nieuwe risico's en kansen met betrekking tot Artifical Intelligence (AI), algoritmes en ChatGTP. Gebruik van deze nieuwe technieken moet een bewuste keuze zijn. Het moet ook inzichtelijk zijn wanneer deze technieken gebruikt worden. Van geval tot geval moet onderzocht worden of gebruik van AI wenselijk is. Hiervoor moet de gemeente beleid opstellen en samenhangende procedures. Met behulp van een DPIA (Data Privacy Impact As-sessment) of een ethische toets kunnen we analyses op processen uitvoeren. Zo bepalen we het de nieuwe techniek gaan gebruiken en welke maatregelen genomen moeten worden om de bij dit pro-ces behorende risico's naar een acceptabel niveau terug te brengen. Dit soort analyses worden bij voorkeur bij proceswijzigingen of implementatie van het proces uitgevoerd.

Algoritmes kunnen helpen bij beoordelen of je voldoet aan gestelde voorwaarden. Ook kunnen ze gebruikt worden voor herkennen van trends. Om transparant te maken welke algoritmes we als overheid gebruiken, worden deze in het landelijk Algoritmeregister gepubliceerd.
Westland sluit aan bij het landelijk register. Volgens de richtlijnen publiceert Westland algoritmes als deze impactvol zijn.

6. Verantwoordelijkheden

Het gegevensbeschermingsbeleid beschrijft aan welke eisen de gemeente vanuit wet- en regelge-ving op het gebied van gegevensbescherming moet voldoen. Voor de borging van het beleid is het van belang diverse taken, verantwoordelijkheden en bevoegdheden goed in de organisatie te beleg-gen.

6.1 Verantwoordelijkheidsniveaus binnen de organisatie

Binnen de organisatie onderscheiden wij (in lijn met geldende wet- en regelgeving) de volgende verantwoordelijkheids- en takenniveaus met betrekking tot gegevensbescherming:

College van B&W
Het college stelt formeel het gegevensbeschermingsbeleid vast. Het college delegeert de uitvoering hiervan en informeert de raad periodiek over dit thema. Binnen het college valt gegevensbescher-ming onder de portefeuille van een van de portefeuillehouders. De directie adviseert het college formeel over het vast te stellen beleid.

Concerndirectie
De directie geeft sturing aan de uitvoering van het gegevensbeschermingsbeleid en ziet erop toe dat naleving van dit beleid plaatsvindt. De directie zorgt dat voor elk werkproces een proceseigenaar is benoemd die verantwoordelijk is voor de informatiebeveiliging en privacy van het werkproces.
De directie zorgt dat de eindverantwoordelijke portefeuillehouders binnen het college gevraagd en ongevraagd geïnformeerd worden over de mate waarin informatiebeveiliging en privacybescherming een onderdeel is van het handelen van de bedrijfsvoering. De directie stelt het gewenste niveau van continuïteit en vertrouwelijkheid vast.

Teammanagers, AON's en proceseigenaren
Zij zijn eigenaar van en integraal verantwoordelijk voor de (informatie)veiligheid en privacy van de informatieprocessen en -systemen binnen hun organisatieonderdeel.
Zij rapporteren aan de directie over de door hen tactisch en operationeel uitgevoerde informatiebeveiligings- en privacybeschermende activiteiten.

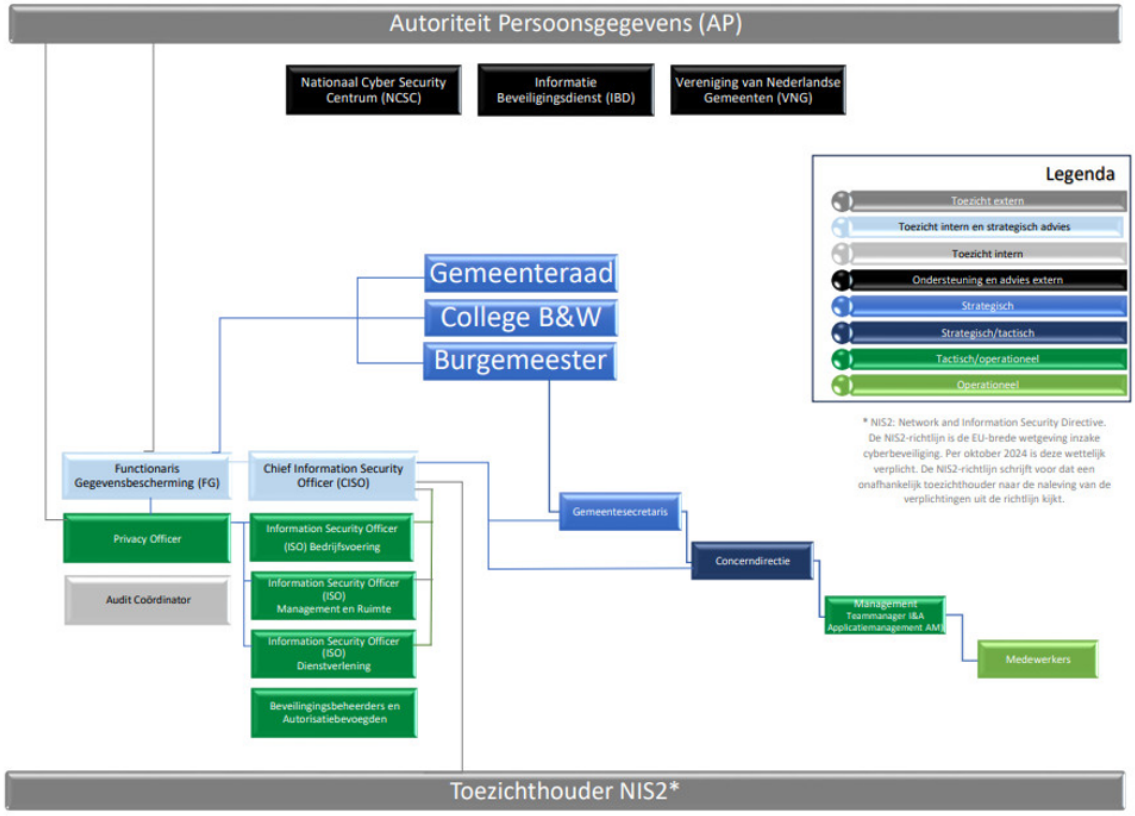
Medewerkers
Alle medewerkers dragen verantwoordelijkheid voor de veiligheid van de activiteiten die behoren tot hun eigen functie en taken. Ze gaan zorgvuldig om met informatie en (informatie)systemen.

Functionaris Gegevensbescherming (FG)
De FG is conform de AVG de interne, onafhankelijke toezichthouder op de verwerking van persoonsgegevens binnen de organisatie. De FG heeft de volgende kerntaken (AVG art 39), vertaald naar de situatie bij de organisatie:
1. Adviseren
2. Toezien op naleving
3. Samenwerken met en contactpunt zijn van de Autoriteit Persoonsgegevens (AP)
4. Optreden als contactpunt voor betrokkenen

Privacy Officer (PO)
De rol van PO is gericht op de coördinatie, uitvoering en naleving van de AVG. Deze functionaris adviseert de organisatie over privacybescherming en over activiteiten ter bescherming van per-soonsgegevens in het kader van de AVG en BIO. Ook is de PO verantwoordelijk voor het beheersen van risico's op privacy en AVG.

Chief Information Security Officer (CISO)
De CISO is op basis van een vastgesteld profiel aangewezen door de directie. Deze rol is namens de directie op strategisch en organisatieniveau verantwoordelijk voor het actueel (laten) houden van het gegevensbeschermingsbeleid, het (laten) coördineren van de uitvoering van het beleid, het beheer-sen van risico's overeenkomstig de behoeften en de risicobereidheid van de organisatie, evenals het rapporteren aan college en directie.

Information Security Officers (ISO's)
De ISO's ondersteunen de CISO en de PO.
Deze rol is op tactisch en eenheidsniveau verantwoordelijk voor het coördineren van de uitvoering van het beleid, het adviseren bij projecten en het beheersen van risico's.



7. Ketensamenwerking

Als overheid is digitale gegevensuitwisseling met ketenpartners of samenwerkingsverbanden een actueel gegeven. Bij gemeenten ontstaat het toenemende bewustzijn dat zij aan inwoners, onderne-mers en ketenpartners verplicht zijn hun verantwoordelijkheid te nemen in de digitale samenleving. Bestuurders streven naar een verdere verhoging van de digitale weerbaarheid in brede zin: in de eigen organisatie, bij ketenpartners en voor inwoners en ondernemers. Dat betekent dat permanent aandacht besteed wordt aan digitale veiligheid bij bestuur en ambtenaren.
De organisatie staat open voor samenwerking met ketenpartners en regionaal met gemeenten en in Gemeenschappelijke Regelingen. Voor het begin van een mogelijke samenwerking maken we heldere afspraken over het doel van de samenwerking en de passende gegevensbescherming. En stellen we vast hoe we de toegang tot de gegevens regelen. Dit betekent dat risico's en noodzakelijke maat-regelen aantoonbaar meewegen in keuzes van samenwerking en bij het aangaan van contracten.
De gemeentelijke organisatie werkt met heel veel gegevens, die soms zeer privacygevoelig of bedrijfsgevoelig zijn. Door de toenemende ketensamenwerking worden deze gegevens steeds vaker gedeeld met ketenpartners. Op technisch vlak moeten wij als gemeente kunnen vertrouwen op de ICT-voorzieningen van de partijen waarmee we gegevens uitwisselen. Met betrekking tot de opslag van informatie of de uitvoering van bedrijfsprocessen. En de ketenpartners moeten uiteraard ook op ons kunnen vertrouwen.

Een inwoner moet erop kunnen vertrouwen dat de gemeente en ketenpartners zorgvuldig omgaan met zijn/haar gegevens en dat niet zomaar iedereen toegang heeft tot deze gegevens. De overheid in het

bijzonder heeft een belangrijke taak de privacy van de inwoners te waarborgen. Dit is de reden dat we de gegevensbeschermingsrisico's identificeren en maatregelen toepassen die horen bij de gegevensverwerking en de verantwoordelijkheid van de partners.

8. Borging en naleving

Om de borging van het beleid en de daarvan afgeleide plannen te realiseren, worden bepaalde rol-len toebedeeld en de Plan, Do, Check, Act (PDCA) cyclus doorlopen. We hanteren onderstaande uit-gangspunten voor het doorlopen van deze PDCA-cyclus. Het doorlopen van de cyclus resulteert in een Information Security Management System (ISMS) en een Privacy Management System (PMS).

Het beleid op de informatieveiligheid en privacy (zowel strategisch als tactisch)
Dit is een organisatie breed, integraal beleid dat de uitgangspunten, de normen en de kaders biedt voor de veiligheid van alle onderliggende informatieprocessen. Uitzonderingen hierop zijn toege-staan, maar dan wel duidelijk gemotiveerd én verifieerbaar. Dit wordt ook wel het 'pas toe of leg uit' principe genoemd. Beoordeling en actualisatie van het gegevensbeschermingsbeleid vindt periodiek plaats (minimaal 1x per drie jaar) en in aansluiting bij de (bestaande) bestuurs- en P&C-cycli en ex-terne ontwikkelingen.

Analyse van de informatieveiligheid en privacy
Dit uitgangspunt is gericht op de invoering. Dit begint met een informatieveiligheids- en privacy analyse. Er wordt allereerst een overzicht opgesteld van alle informatiesystemen en gegevensverzamelingen in de organisatie. De informatiesystemen en gegevensverzamelingen worden toegewezen aan een eigenaar en geclassificeerd op de risicoklassen Beschikbaarheid, Integriteit en Vertrouwelijk-heid van de informatie ("dataclassificatie").
Ook wordt het Basis Beveiligingsniveau (BBN) per informatiesysteem vastgesteld. Om risicomana-gement hanteerbaar en efficiënt te houden, kiest de BIO voor een diepgang van de uitwerking van het risicomanagement die proportioneel is aan de te beschermen belangen in combinatie met rele-vante dreigingen. Daarom onderscheidt de BIO drie basisbeveiligingsniveaus (BBN's):

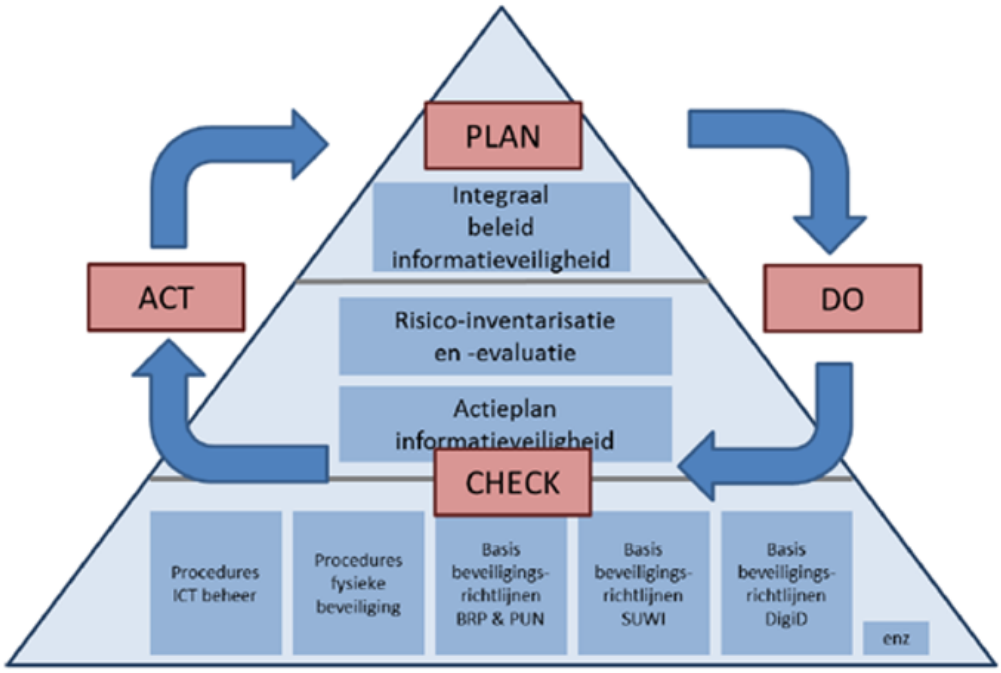
1. Voor BBN1 ligt de nadruk op 'wat mag minimaal verwacht worden?';
2. Voor BBN2 ligt de nadruk op de bescherming van de meest voorkomende categorieën informatie volgens het principe 'Valt de maatregel onder goed huis- vaderschap? Toont deze beveiliging de betrouwbare overheid?'. Vrijwel alle informatie(systemen) van de gemeentelijke organisatie valt bin-nen dit niveau;
3. BBN2+ is in het leven geroepen voor gemeenten. BBN2 is bij sommige processen niet voldoende. En BBN3 is van toepassing op categorieën informatie met de classificatie staatsgeheim. Gemeenten beheren geen staatsgeheimen, maar BBN2 is soms net niet voldoende. BBN2+is daarom in het le-ven geroepen omdat het voor gemeenten soms noodzakelijk is om aanvullende maatregelen te ne-men boven BBN2. Samen met gemeenten is er een passende set van maatregelen bovenop BBN2 opgesteld.

Bij de gemeentelijke organisatie vallen vrijwel alle informatiesystemen en gegevens onder niveau BBN2. Hiervan kan bij individuele informatiesystemen worden afgeweken met een goede (vastge-legde) onderbouwing. Hierna wordt de praktijksituatie in de organisatie getoetst aan het organisatie brede veiligheidsbeleid en aan de beveiligingsmaatregelen uit de BIO en AVG. Dit wordt gedaan door het uitvoeren van een risico-inventarisatie en evaluatie (RI&E), GAP-analyse, rondgang van het gebouw en een (eventuele) evaluatie van het vorige actieplan. Bij een Gap analyse vergelijk je de huidige situatie met de verwachte of gewenste situatie door het stellen van 3 vragen:
Waar zijn we?; Waar willen we heen?; Hoe gaan we daar komen?
Bijstelling van de informatieveiligheid- en privacy analyse vindt elk jaar plaats.

Actieplan Informatieveiligheid en privacy
Op basis van de informatieveiligheids- en privacy analyses die eerder genoemd werden, worden actieplannen opgesteld. De geconstateerde risico's worden gewogen en waar nodig van maatregelen voorzien.
Prioritering van de acties wordt gedaan op basis van de grootte van het risico. Hierbij worden ook zaken als geaccepteerde- en restrisico's besproken.
Hierdoor ontstaat een compact actieplan waarmee de organisatie vaststelt welke verbeteracties gedurende een periode van één of twee jaar worden uitgevoerd. Dit actieplan vormt een praktische leidraad voor de verbetering en borging van informatieveiligheid en privacy in de organisatie. De informatieveiligheids- en privacy organisatie komt bij elkaar om de implementatie van het actieplan te evalueren, te bewaken en waar nodig bij te stellen. Dit wordt minimaal driemaal per jaar bespro-ken in het Team Gegevensbescherming.

Technische en organisatorische maatregelen

Dit uitgangspunt bestaat uit het opleveren van een complete set aan organisatorische, technische en fysieke maatregelen die gericht zijn op de specifieke eisen van een onderdeel. Het kan gaan om maatregelen uit de BIO en AVG, maar ook om de primaire processen van de organisatie, applicaties (zoals bij burgerzaken of het Sociaal Domein), de basisregistraties, het financiële systeem, proces-sen omtrent het Informatiebeheer, ICT-beheerprocessen of de fysieke beveiliging van het gebouw. Dit betreft vooral het opstellen van procedures en werkinstructies.
Om te beoordelen of de organisatie de doelstellingen uit het beleid heeft behaald, worden periodie-ke onafhankelijke audits en controles uitgevoerd. Bij een audit toetst een onafhankelijke deskundige partij op de opzet, bestaan en werking van beheersmaatregelen. Hiervoor kan een externe (erkende) partij worden ingeschakeld. Jaarlijks wordt een auditplan (intern controleplan) opgesteld waarin wordt vastgelegd welke interne controles en audits in het komende jaar plaatsvinden en op welke informatiesystemen deze betrekking hebben. In dit plan wordt tevens een beschrijving van de uit te voeren controles opgenomen, evenals de uitvoerders en verantwoordelijken (lijnniveau) voor de con-troles gekoppeld aan een tijdsplanning. Ook de jaarlijkse controle op de technische naleving van beveiligingsnormen bij informatiesystemen, zoals penetratietesten, zijn onderdeel van dit plan. De resultaten van de uitgevoerde audits worden, namens de lijnverantwoordelijken, gerapporteerd aan de CISO en FG. De CISO en FG bundelen deze resultaten en rapporteren hierover periodiek aan de directie.



Aldus besloten door de raad in zijn openbare vergadering van 27 maart 2024 ,

de griffier
P. van Oosten

de voorzitter
B.R. Arends