gemeente wageningen

GEMEENTEBLAD

Officiële uitgave van de gemeente Wageningen

Nr. 32624

26 januari

2022

Strategisch Gegevensbeschermingsbeleid Gemeente Wageningen 2022 tot 2025

1. Inleiding

Deze beleidsnota beschrijft het strategisch Gegevensbeschermingsbeleid voor de jaren 2022 tot 2025 en vervangt het in 2019 vastgestelde 'Beleid informatieveiligheid en privacy 2019'.
Deze beleidsnota is richtinggevend en kaderstellend en wordt aangevuld met een jaarlijks te schrijven informatiebeveiligingsplan en een privacyplan. Die twee plannen geven op hoofdlijnen invulling aan de gegevensbescherming van gemeente Wageningen en worden ieder jaar aangevuld door zes team-specifieke deelplannen. Verder worden werkafspraken en richtlijnen opgesteld voor de uitwerking van specifieke onderwerpen, waaronder datalekken, toegangsbeveiliging en SUWINET.

Met dit 'Strategisch Gemeentelijk Gegevensbeschermingsbeleid 2022 tot 2025 zet de gemeente een volgende stap in de bescherming van persoonsgegevens en andere gegevens binnen de gemeente en bouwt daarbij voort op de stappen die in de voorgaande jaren gezet zijn. De beleidstermijn loopt tot 2025. Hierdoor kan voorafgaande de nieuwe raadsperiode een evaluatie van het beleid plaatsvinden. Noodzakelijke verbeteringen kunnen vervolgens in de nieuwe raadsperiode worden verwerkt.

1.1 Leeswijzer

Hoofdstuk 1 van dit Gegevensbeschermingsbeleid introduceert de onderwerpen privacy en informatiebeveiliging in de context van gemeente Wageningen. De visie van gemeente Wageningen op gegevensbescherming staat beschreven. Ook de vier ambities voor de komende beleidsperiode zijn in het eerste hoofdstuk geformuleerd. In hoofdstuk 2 wordt de kern van het strategisch beleid uiteengezet. De scope en de plaats van het strategisch beleid staan beschreven. Evenals de ontwikkelingen die relevant zijn voor het actualiseren van het beleid en de uitgangspunten die gelden voor privacy en informatiebeveiliging. Daarnaast introduceert het tweede hoofdstuk de randvoorwaarden die noodzakelijk zijn voor het behalen van de doelen uit het strategisch beleid. Hoofdstuk 3 beschrijft hoe de taken en verantwoordelijkheden in de organisatie zijn belegd. Hierbij komen het college van B en W, de directie, het MT en de teammanager aan bod. Tot slot staat de wijze waarop controle en verantwoording plaatsvinden beschreven.

1.2 Bescherming van gegevens

Het Gegevensbeschermingsbeleid geldt voor alle processen van de gemeente en alle handelingen van de gemeente waarin persoonsgegevens en andere gegevens worden verzameld, verwerkt en gedeeld. Het beleid borgt daarmee de informatiebeveiliging en privacy gedurende de hele levenscyclus van informatiesystemen en de hele levenscyclus van gegevens, ongeacht de toegepaste technologie en ongeacht het karakter van de gegevens. Het beperkt zich niet alleen tot de ICT en heeft betrekking op het politieke bestuur, alle medewerkers, inwoners, klanten, gasten, bezoekers en externe relaties.

1.2.1 Wat is 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 gegevens. Het begrip 'aantoonbaar' betekent dat de gemeente kan bewijzen dat de beveiligingsmaatregelen zijn beschreven, uitgevoerd worden, en over een langere periode hebben gewerkt.

Beschikbaarheid	De mate waarin gegevens en gegevensverwerkingen op de juiste momenten beschikbaar zijn voor gebruikers.
Integriteit	De mate waarin de juistheid en volledigheid van gegevens is gewaarborgd.
Vertrouwelijkheid	De mate waarin gegevens alleen toegankelijk zijn voor degenen die hiervoor gerechtigd zijn.

1.2.2. Wat is Privacy?

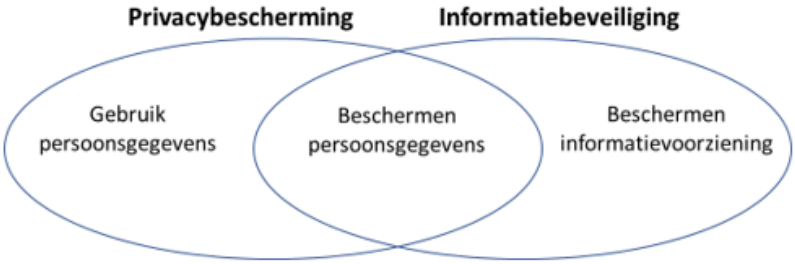
Onder Privacy wordt verstaan de bescherming van persoonsgegevens. Met persoonsgegevens wordt bedoeld de informatie die – al dan niet met enige moeite - herleid kan worden tot individuele personen. Privacy is verankerd in de Grondwet en verder uitgewerkt in o.a. de Algemene verordening gegevensbescherming (AVG), de Uitvoeringswet AVG (UAVG) en de wet Politiegegevens (Wpg). Binnen de gemeente is een Functionaris gegevensbescherming (FG)[1] aangesteld die toeziet op de bescherming van

1) FG staat voor Functionaris Gegevensbescherming, een wettelijke functie o.b.v. AVG en Wpg. De FG houdt toezicht.

persoonsgegevens. Ook de nationale toezichthouder, de Autoriteit Persoonsgegevens, ziet toe op de bescherming van persoonsgegevens. Privacy werkt vanuit een aantal generieke principes. Die zijn weergegeven in bijlage A.

1.2.2 Samenhang privacy en informatiebeveiliging

De privacywetgeving stelt eisen aan het gebruik en de beveiliging van persoonsgegevens. De regels voor het gebruik geven richting aan alle verwerkingen[2] die met persoonsgegevens worden uitgevoerd en de uitwisseling van persoonsgegevens met andere partijen. De beveiligingseisen dienen de persoonsgegevens te beschermen en hun beschikbaarheid, integriteit en vertrouwelijkheid te waarborgen. Dit komt overeen met de doelstellingen van informatiebeveiliging. Informatiebeveiliging beschermt behalve persoonsgegevens ook de andere gegevens en gegevensstromen binnen de gemeente. Hieronder is dit schematisch weergegeven. De samenhang tussen de werkzaamheden van de privacy- en beveiligingsfuncties binnen de gemeente, wordt hiermee duidelijk.



Samenhang privacybescherming en informatiebeveiliging

1.3 Ambitie en visie van de gemeente

De gemeente Wageningen staat midden in de samenleving. De omvang van haar dienstverlening is in de afgelopen jaren flink toegenomen. Ze heeft meer taken gekregen en de interactie tussen inwoners, de gemeente en haar (keten)partners is steeds diverser en omvangrijker geworden. Vanwege deze interacties en de toenemende digitalisering is de kwaliteit van de informatie nog belangrijker voor een goede bedrijfsvoering en dienstverlening. Die kwaliteit steunt op het goed borgen van de beschikbaarheid, integriteit en vertrouwelijkheid van informatie. Daarnaast heeft zich een vorm van criminaliteit ontwikkeld met als bedrijfsmodel geld verdienen aan het ontwrichten van de informatievoorziening en het gijzelen en verkopen van (persoons)gegevens. De omvang en de impact van deze criminaliteit zijn aanzienlijk.

Wageningen is zich bewust van deze maatschappelijke ontwikkelingen en realiseert zich eveneens dat zij een belangrijke rol speelt in het beschermen van de informatie die haar is toevertrouwd door haar inwoners, ondernemers en (keten)partners. Zij heeft een monopoliepositie. De inwoner kan immers niet naar een andere gemeente voor haar dienstverlening. Daarnaast dient de gemeente een belangrijk maatschappelijk belang, omdat zij in haar optreden en uitvoering het gezicht is van de betrouwbare overheid. In het Wageningse dienstverleningsconcept[3] heeft de gemeente de ambitie geuit om te werken met veilige, betrouwbare systemen waarmee de privacy is beschermd.

Gemeente Wageningen heeft in de afgelopen jaren al veel energie gestoken in het op niveau brengen van haar informatiebeveiliging, het inrichten van de informatiebeveiligingsorganisatie en het uitvoeren van verbeterplannen. Dit is een continu (verbeter)proces, omdat haar dienstverlening en de informatiebeveiligingsrisico's veranderen. Voor de komende beleidsperiode heeft de Gemeente Wageningen in haar Gegevensbeschermingsbeleid 2022-2025 vier ambities geformuleerd, namelijk:

1. **BIO op orde.**
   De Baseline Informatiebeveiliging Overheid is sinds 2019 verplicht binnen de overheid. De BIO kent verplichte overheidsmaatregelen die zijn gedefinieerd om de gemeenten:
   a) Te laten voldoen aan de geldende wet- en regelgeving.

2) De term verwerking is in de AVG gedefinieerd als 'een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens'.

3) https://wageningen.raadsinformatie.nl/document/10088279/2#search=%22dienstverleningsconcept%22

b) Te laten voldoen aan minimale beheerstandaarden voor een betrouwbare en veilige informatievoorziening.
c) Een praktische invulling te laten geven aan de gemeenschappelijke veiligheid van informatieketens.

Er moet nog veel gebeuren aan de implementatie van de BIO. Als eerste ambitie leggen we neer dat de BIO overheidsmaatregelen geïmplementeerd zijn op BBN2 niveau[4] en aantoonbaar effectief zijn. Over de effectiviteit van maatregelen wordt feitelijk gerapporteerd, zodat een accuraat beeld ontstaat over de stand van zaken. Als een overheidsmaatregel niet geïmplementeerd is, dan ligt daar een bewuste en gemotiveerde keuze aan ten grondslag.

2. **Privacy op orde.**
Dit houdt in dat de gemeente de principes van de privacywetgeving volgt (zie 2.4) en haar organisatie en processen hierop heeft ingericht. Dat de privacyfuncties in staat zijn hun werk te doen en de privacyprocessen in opzet aanwezig, afdoende geïmplementeerd en effectief zijn. Zodat de gemeente voldoet aan de wettelijke vereisten van de AVG, de UAVG en Wpg. Deze wetgeving is sinds 2018 verplicht.
De kernprocessen zijn:
a) Opstellen, implementeren en onderhouden van het privacy beleid en gedragsregels.
b) Geven van voorlichting over privacy en verhogen van de bewustwording.
c) Implementeren en onderhouden van een Register van verwerkingsactiviteiten.
d) Uitvoeren van de Meldplicht Datalekken, inclusief registratie en rapportage.
e) Uitvoeren van privacyanalyses (DPIA's) voor projecten en bestaande verwerkingen.
f) Afsluiten en managen van verwerkersovereenkomsten.
g) Uitvoeren van de rechten van betrokkenen, inclusief registratie en rapportageprocessen.
h) Transparantie realiseren en borgen, door privacyverklaringen op te stellen.
i) Borgen van Privacy by Design en Privacy by Default[5] bij het ontwerp van processen en informatiesystemen.
j) Rapportage over de uitvoering van deze processen aan de FG, het management, het bestuur en desgevraagd bij de Autoriteit Persoonsgegevens.

3. **De bezetting op orde.**
Gegevensbescherming is een integraal onderdeel van de kwaliteit van werken van de gemeente. Zij vergt aandacht en inzet van alle organisatieonderdelen van de gemeente. In de huidige situatie is de vaste bezetting gerealiseerd op basis van een drietal deeltijdfuncties, de FG, de privacy officer en de CISO[6]. Deze bezetting komt niet overeen met de uitdagingen die er nog zijn. Gemeente Wageningen heeft behoefte aan een betere invulling van de personele bezetting voor privacy en informatiebeveiliging. Dit omvat specialistische functies, bijvoorbeeld een Technical Security Specialist die de organisatie adviseert over de beveiliging van het netwerk en de componenten van de ICT-infrastructuur om zo de continuïteit en veiligheid van digitale en online toepassingen te verbeteren, of een functionaris die structureel de uitvoerende beveiligingswerkzaamheden voor Suwinet verricht. Maar het omvat ook contactpersonen en inzet binnen alle teams. Zodat er voldoende aandacht is voor gegevensbescherming en alle verplichtingen worden ingevuld en gedragen.

4. **Zelf leren op orde.**
Zelflerend vermogen is belangrijk voor de ontwikkeling van privacy en informatiebeveiliging binnen Wageningen. Door te leren borgt en verbetert de gemeente haar kennis en vaardigheden. Ook is dit leervermogen nodig om de resultaten en leerpunten van de ENSIA zelfevaluaties en ENSIA audits om te zetten naar gerichte verbeteracties. De gemeente wil inzetten op duidelijker eigenaarschap voor verbeteracties en een beter proces opzetten voor het doorlopen van de kwaliteitscyclus, de Plan, Do, Check, Act cyclus (PDCA). De cyclus zal structureel geborgd en verder geautomatiseerd worden.

4) BBN2 staat voor het middenniveau van beveiligingsmaatregelen. Dit is het 'oude' niveau van de 'Baseline Informatiebeveiliging Gemeenten' en tevens het standaardniveau voor de uitwisseling tussen overheidspartijen. Ook is BBN2 het standaardniveau om te voldoen aan de wettelijke eisen uit onder meer de wetten voor de basisadministraties.
5) Een toelichting van de begrippen Privacy by Design en Privacy by Default is te vinden in bijlage A.
6) De privacy officer is de uitvoerende functie op het gebied van privacy. CISO staat voor Concern Information Security Officer, deze voert de toezichts- en regiefunctie voor informatiebeveiliging.

2. Strategisch beleid

2.1 Doel

Het doel van deze beleidsnota is het presenteren van het 'Strategisch Gegevensbeschermingsbeleid voor de jaren 2022 tot 2025. De uitwerking van dit beleid in concrete maatregelen vindt plaats in het jaarlijks bij te stellen informatiebeveiligingsplan en het jaarlijks bij te stellen privacyplan.

2.2 Ontwikkelingen

De ontwikkelingen die van belang zijn voor de actualisering van het Gegevensbeschermingsbeleid zijn de volgende:

2.2.1 De BIO

De BIO (Baseline Informatiebeveiliging Overheid) is sinds 2019 het normenkader voor de gehele overheid. De werkwijze van deze BIO is gericht op risicomanagement met de inzet van verplichte overheidsmaatregelen. Deze verplichte maatregelen zijn ontworpen en geselecteerd uit de ISO27001/2.
Sinds de BIO van kracht is, zal het bestuur en het managementteam (MT) meer dan vroeger moeten werken volgens de aanpak van de ISO 27001. Daarbij is risicomanagement van belang. Dit houdt in, dat men op voorhand keuzes maakt en continu afwegingen maakt of gegevens in bestaande en nieuwe processen adequaat beveiligd zijn in termen van beschikbaarheid, integriteit en vertrouwelijkheid. Maatregelen moeten aantoonbaar worden ingericht en uitgevoerd.

2.2.2 Dreigingsbeeld Nederlandse Gemeenten en Agenda Digitale Veiligheid 2020-2024

Het Dreigingsbeeld Nederlandse Gemeenten geeft een actueel zicht op incidenten en factoren uit het verleden, aangevuld met een verwachting voor het heden en de nabije toekomst. Het dreigingsbeeld is een bouwsteen van de Agenda Digitale Veiligheid 2020-2024 en geeft de onderbouwing voor strategische handelingsperspectief van de gemeenten.

2.2.3 Documenten ter verbetering

De Autoriteit Persoonsgegevens, de VNG, de Informatie Beveiligingsdienst (IBD) en de onafhankelijk functionerende FG leveren continue aanbevelingen en producten ter verbetering van de bescherming van persoonsgegevens. Deze producten zijn ideaal voor het aanbrengen van focus in de actualisatie van beleid en plannen voor Privacy.

2.2.4 Informatie uit incidenten en datalekken

De gemeente kent naast het hierboven genoemde dreigingsbeeld natuurlijk een eigen systeem waarin incidenten en datalekken 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.

2.2.5 De 10 principes voor informatiebeveiliging

De 10 principes voor informatiebeveiliging zijn een aanvulling op het normenkader[7] BIO en gaan over de waarden die de bestuurders en managers zichzelf opleggen. De principes gaan vooral over de rol bij het borgen van informatiebeveiliging in de gemeentelijke organisatie. Deze principes ondersteunen de bestuurders en managers bij het uitvoeren van goed risicomanagement. Als er iets verkeerd gaat met betrekking tot het beveiligen van de gegevens binnen de gemeentelijke processen, dan kan dit directe gevolgen hebben voor inwoners, ondernemers en partners van de gemeente. Daarmee is het onderwerp informatiebeveiliging nadrukkelijk gewenst op de bestuurs- en managementtafels. De uitwerking van de principes vindt op later moment, in overleg met de bestuurders en het MT, plaats.
De principes zijn als volgt:

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

7) Deze principes zijn gelijktijdig met de BIO gepubliceerd, zie besluitvorming Informatiebeveiligingsdienst (IBD) en Verenigde Nederlandse Gemeenten (VNG)

2.3 Standaarden informatiebeveiliging
Informatiebeveiligingsmaatregelen worden genomen op basis van best practices bij (lokale) overheden en NEN-ISO/IEC 27002:2017. De basis voor de inrichting van onderhavig beleid is NEN-ISO/IEC 27001:2017.
Voor de ondersteuning van gemeenten bij het formuleren en realiseren van hun informatiebeveiligingsbeleid heeft de interbestuurlijke werkgroep Normatiek[8] in 2018 de Baseline Informatiebeveiliging Overheid (BIO) uitgebracht. De BIO bestaat uit een baseline met verschillende niveaus van beveiligen.

De praktische handreikingen van de IBD[9] volgen de inhoud en de structuur van de BIO en de ISO. Bij het opstellen van het informatiebeveiligingsplan en bij interne werkafspraken of interne richtlijnen kunnen de praktische handreikingen van de IBD als voorbeeld fungeren.

2.4 Standaarden bescherming van persoonsgegevens
De AVG en de UAVG bieden de wettelijke uitgangspunten voor ons privacybeleid. Zo bepaalt de AVG in artikel 5 enkele principes waar de gemeente aantoonbaar aan moet voldoen. In bijlage A staan deze principes verder uitgewerkt.
1. Persoonsgegevens dienen rechtmatig, behoorlijk en transparant te worden verwerkt.
2. Persoonsgegevens worden verwerkt met een duidelijk doel.
3. Uitsluitend de noodzakelijke persoonsgegevens worden verwerkt.
4. Persoonsgegevens moeten actueel en juist gehouden worden.
5. Uitsluitend noodzakelijke persoonsgegevens worden bewaard.
6. Persoonsgegevens worden beveiligd.

2.5 Plaats van het strategisch beleid
Het strategisch beleid wordt gebruikt om de basis te leggen voor het jaarlijks te schrijven 'Gemeentelijk Informatiebeveiligingsplan' en het 'Gemeentelijk Privacyplan', waarmee richting wordt gegeven aan de verdere invulling van informatiebeveiliging en privacy op tactisch en operationeel niveau. Het informatiebeveiligingsplan wordt op hoofdlijnen opgesteld onder leiding van de CISO. De inhoud van het informatiebeveiligingsplan is gebaseerd op:
- De uitkomsten van de jaarlijkse Eenduidige Normatiek Single Information Audit (ENSIA);
- Het dreigingsbeeld gemeenten van de IBD en het implementeren van de Agenda Digitale Veiligheid 2020-2024;
- De door de teammanagers ingebrachte onderwerpen voor de informatievoorziening waarvoor zij verantwoordelijk zijn, bijvoorbeeld als uitkomst van een risicoanalyse;
- Landelijke ontwikkelingen en nieuwe wetgeving;
- Uitkomsten van (financiële) audits en interim controles die zijn gericht op informatiebeveiliging.

Het privacyplan wordt opgesteld onder leiding van de privacy officer en is gebaseerd op:
- De uitkomsten en aanbevelingen van de jaarlijkse FG-meting;
- Aanbevelingen van de VNG & IBD;
- Aanbevelingen van de Autoriteit Persoonsgegevens;
- De door teammanagers ingebrachte onderwerpen voor het privacyplan. Denk aan de uitkomsten van een risicoanalyse (DPIA);
- Uitkomsten van de (financiële) audits en interim controles die zijn gericht op privacy.

De gemeentelijke jaarplannen worden aangevuld met team-specifieke deelplannen. Deze team specifieke deelplannen worden jaarlijks opgesteld door iedere teammanager. Hierin staan de concrete acties en de planning vermeld, om de praktijk in overeenstemming te brengen met datgene wat in het beleid is afgesproken.
Ook worden er onderwerp specifieke werkinstructies en richtlijnen opgesteld. Daarin worden de werkafspraken uitgewerkt voor specifieke onderwerpen, zoals BAG, Wpg, en SUWINET.

2.6 Scope informatiebeveiliging en privacy
De scope van dit beleid omvat alle gemeentelijke processen, (persoons- en politie)gegevens, onderliggende informatiesystemen, procesautomatisering, informatie en gegevens van de gemeente en externe partijen (bijvoorbeeld politie), het gebruik daarvan door medewerkers en (keten)partners in de meest brede zin van het woord, ongeacht locatie, tijdstip en gebruikte apparatuur. Het Gegevensbeschermingsbeleid dekt ook aanvullende beveiligingseisen uit wetgeving af zoals voor de BRP, PNIK en SUWI. Voor bepaalde kerntaken gelden bovendien nog enkele specifieke (aanvullende) beveiligingseisen (bijvoorbeeld SUWI en gemeentelijke basisregistraties). Deze worden in aanvullende werkinstructies en richtlijnen

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

geformuleerd. Bewust wordt in het strategisch beleid geen limitatief overzicht van onderliggende documenten opgenomen. In de onderliggende documenten wordt de link naar het strategisch beleid gelegd.

2.7 Uitgangspunten
Het bestuur, de directie en het managementteam spelen een cruciale rol bij het uitvoeren van dit 'Strategische Gegevensbeschermingsbeleid'. Zij geven een duidelijke richting aan informatiebeveiliging en privacy en demonstreren dat zij informatiebeveiliging en privacy ondersteunen en zich hierbij betrokken voelen, door het uitdragen en handhaven van een Gegevensbeschermingsbeleid van en voor de hele gemeente.

2.7.1 Strategische doelen
De strategische hoofddoelen van het Gegevensbeschermingsbeleid 2022 – 2025 zijn:
- Het waarborgen van het democratische proces en de democratische besluitvorming van de gemeente Wageningen.
- Het waarborgen van dienstverlening aan de inwoners, ondernemers en overige belanghebbenden van de gemeente Wageningen.
- Het beschermen van de (persoons)gegevens van de inwoners, ondernemers en overige belanghebbenden van de gemeente Wageningen

Deze strategische doelen zijn uitgewerkt in de volgende concrete doelen voor het Gegevensbeschermingsbeleid:
- Het voldoen aan wet- en regelgeving, zoals AVG, UAVG en Wpg.
- Het beschermen en correct verwerken van (persoons)gegevens.
- Adequate bescherming van bedrijfsmiddelen en bedrijfsprocessen.
- 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 verwerking en veilige informatiesystemen.
- Het adequaat reageren op incidenten en datalekken.

2.7.2 Belangrijkste uitgangspunten
De belangrijkste uitgangspunten van het beleid zijn:
- Het college van B en W is eindverantwoordelijk voor de gegevensbescherming en stelt het strategisch Gegevensbeschermingsbeleid vast. Het beleid wordt eens per 4 jaar bijgesteld.
- Gegevensbescherming is een continu verbeterproces. 'Plan, do, check en act' vormen samen het managementsysteem van beheersing. Door periodieke controle, organisatiebrede planning én coördinatie wordt de kwaliteit van privacy en informatiebeveiliging verankerd binnen de organisatie.
- Informatiebeveiliging en privacy zijn niet uitsluitend ICT gerelateerd. Ook menselijk gedrag en de fysieke toegangsbeveiliging van alle gemeentelijke gebouwen vormen belangrijke onderdelen van gegevensbescherming.
- 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.
- Gegevensbescherming wordt in de gemeente Wageningen gezien als een integraal onderdeel van risicomanagement. Dit betekent dat de maatregelen in het kader van informatiebeveiliging en privacy op basis van risicoanalyses worden geselecteerd en ingevoerd.
- Bijzondere persoonsgegevens, bijvoorbeeld gegevens over gezondheid, politiegegevens, of gegevens waaruit etnische afkomst blijkt, vragen extra beheersingsmaatregelen van de organisatie.
- Alle medewerkers van de gemeente worden getraind in het gebruik van beveiligingsprocedures, op de procedures voor het afhandelen van informatiebeveiligingsincidenten en datalekken en in het correct omgaan met persoonsgegevens.
- De Concern Information Security Officer (CISO) ondersteunt vanuit een onafhankelijke positie de organisatie bij het bewaken en verhogen van de betrouwbaarheid van de informatievoorziening.
- De Functionaris Gegevensbescherming (FG) adviseert en controleert de organisatie vanuit een onafhankelijke positie bij de bescherming van persoonsgegevens.
- De Concern Controller ziet toe op een integrale aanpak van alle onderwerpen binnen de P&C-cyclus.
- De Privacy Officer ondersteunt en adviseert de organisatie bij de bescherming van persoonsgegevens
- Alle processen van de gemeente Wageningen hebben een eigenaar, ook de ketenprocessen. De eigenaar is verantwoordelijk voor de bescherming van de gegevens in het proces.
- De rollen en verantwoordelijkheden voor privacy en informatiebeveiliging worden op duidelijke wijze vastgelegd.

2.7.3 Belangrijkste randvoorwaarden

Het onderhavige Gegevensbeschermingsbeleid kan uitsluitend worden uitgevoerd als wordt voldaan aan de volgende randvoorwaarden.

- De organisatie stelt tijd en middelen beschikbaar om de taken en verantwoordelijkheden op het gebied van informatiebeveiliging en privacy uit te voeren.
- De organisatie heeft voldoende bewustzijn op het gebied van gegevensbescherming en heeft de benodigde kennis en vaardigheden in huis om gegevensbescherming toe te passen.
- Alle (persoons)gegevens en informatiesystemen zijn in beeld. Dat wil zeggen: het eigenaarschap ligt vast en de processen/gegevens/systemen zijn geregistreerd bij ICT of in het register van verwerkingsactiviteiten.

3. Organisatie, taken & verantwoordelijkheden

In dit hoofdstuk wordt uiteengezet welke taken en verantwoordelijkheden met betrekking tot gegevensbescherming op welke plaats belegd zijn binnen de organisatie. De methodiek sluit aan bij de in de bedrijfsvoering bekende Three Lines of Defence (3LoD). In dit model zijn de teammanagers verantwoordelijk voor de eigen processen. De tweede lijn (CISO, security officers en privacy officers) ondersteunt, adviseert, coördineert en bewaakt of het management zijn verantwoordelijkheden ook daadwerkelijk neemt. In de derde lijn wordt het geheel door een (interne) auditor van een objectief oordeel voorzien met mogelijkheden tot verbetering.

3.1 Richting geven en verantwoording afleggen: het college

Met het vaststellen van onderhavig beleid, stelt het college haar ambities op het gebied van gegevensbescherming vast voor de komende jaren. Hiermee geeft zij richting aan privacy en informatiebeveiliging in de gemeente. De ambities staan beschreven in hoofdstuk 1. Het college legt jaarlijks verantwoording af aan de gemeenteraad.

3.2 Aansturing: directie en het MT

De directie zorgt dat alle processen en systemen en de daarbij behorende middelen altijd onder de verantwoordelijkheid vallen van een teammanager. De directie zorgt dat de eindverantwoordelijke portefeuillehouders binnen het college gevraagd en ongevraagd geïnformeerd worden over de staat van de informatiebeveiliging en privacy binnen de organisatie. Op die manier kan het college zich ook verantwoorden aan de raad en andere toezichthouders. De directie stelt het gewenste niveau van continuïteit en vertrouwelijkheid vast.

Het MT zorgt dat de teammanagers zich verantwoorden over de beveiliging van de gegevens. Het MT draagt zorg voor het uitwerken van tactische informatiebeveiligings- en privacybeleidsonderwerpen en laat zich hierin bijstaan door de CISO en de privacy officer van de gemeente. Het MT stelt jaarlijks het informatiebeveiligingsplan en het privacyplan vast. Het MT autoriseert de benodigde procedures en uitvoeringsmaatregelen en is verantwoordelijk voor het (laten) uitwerken van aanvullend beleid en de noodzakelijke werkafspraken, werkinstructies en richtlijnen op organisatieniveau.

3.3 Uitvoering: teammanagers

Informatiebeveiliging en privacy valt onder de verantwoordelijkheden van alle teammanagers. Om deze verantwoordelijkheid waar te maken dienen zij goed ondersteund te worden vanuit de tweede lijn. Teammanagers kunnen hun verantwoordelijkheden niet delegeren. Uitvoerende werkzaamheden kunnen zij wel delegeren. De bedoeling is dat alle processen, systemen, data, applicaties altijd minimaal één eigenaar hebben; er moet dus altijd iemand verantwoordelijk zijn. Teammanagers rapporteren aan het MT over de door hen tactisch en operationeel uitgevoerde gegevensbeschermingsactiviteiten. De teammanagers spreken periodiek met de CISO en privacy officer over gegevensbescherming.

Taken van de teammanagers in het kader van gegevensbescherming zijn:

- Het leveren van input voor wijzigingen op maatregelen en procedures.
- Het voldoen aan wetgeving die op hun processen van toepassing is en invulling geven aan de rollen die binnen die wetgeving bedacht is.
- Het binnen het eigen team uitdragen van het beleid en de daaraan gerelateerde procedures.
- Het vroegtijdig signaleren van de voornaamste bedreigingen waaraan de gegevens zijn blootgesteld.
- Het bespreken van beveiligingsincidenten, datalekken en de consequenties die dit moet hebben voor beleid en maatregelen.
- Het opstellen van het team specifieke deelplan informatiebeveiliging en privacy. Hierin staan de concrete acties van het team vastgelegd om de praktijk in overeenstemming te brengen met datgene wat in het beleid is geëist.

3.4 Controle en verantwoording

Dit Strategisch Beleid is een verantwoordelijkheid van het bestuur van de gemeente Wageningen. De bestuurders en de directie van de gemeente Wageningen zullen richting en sturing geven aan de onderwerpen informatiebeveiliging en privacy door het geven van voorbeeldgedrag en het vragen om informatie.
De directie is verantwoordelijk voor het gevraagd en ongevraagd rapporteren over gegevensbescherming aan de portefeuillehouder. De directie rapporteert daarnaast over de mate waarin zij invulling hebben gegeven aan het uitwerken van tactische (deel) beleidsonderwerpen die aanvullend zijn op dit strategische beleid.

3.4.1 ENSIA

De gemeente verantwoordt zich over informatiebeveiliging met de ENSIA-systematiek. De ENSIA coördinatie maakt onderdeel uit van het takenpakket van de CISO. Deze zorgt ervoor dat de informatie die nodig is voor het beantwoorden van vragen binnen de ENSIA wordt opgehaald bij de verantwoordelijke teammanagers. De teammanagers leveren alle informatie die nodig is voor het invullen van de jaarlijkse ENSIA-vragenlijsten.

De verantwoording over de informatiebeveiliging komt jaarlijks tot uitdrukking in de collegeverklaring Informatiebeveiliging. Met deze verklaring geeft het college van B en W aan in hoeverre de gemeente voldoet aan de afspraken die gemaakt zijn voor de ENSIA-verantwoording Informatiebeveiliging. 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. De collegeverklaring wordt aan de raad aangeboden via een raadsinformatiebrief (RIB). Met deze verantwoording informeert het bestuur van de gemeente Wageningen de gemeenteraad.

3.4.2 Fg -meting

Jaarlijks wordt door de Functionaris Gegevensbescherming een Fg-meting uitgevoerd. In het jaarlijkse rapport van de Fg-meting doet de Functionaris Gegevensbescherming bevindingen en aanbevelingen inzake de bescherming van persoonsgegevens. De aanbevelingen worden aangeboden aan het college van B en W via de portefeuillehouder informatieveiligheid en privacy. De raad wordt jaarlijks geïnformeerd over de bevindingen uit de Fg-meting. Dit gebeurt door middel van een raadsinformatiebrief (RIB).

3.4.3 Overige instrumenten

<u>Inbedding in P&C-cyclus</u>
Gegevensbescherming is onderdeel van het interne beheersingsproces. Het is logisch om alle beheersprocessen zo uniform mogelijk in te richten. Dat schept duidelijkheid en overzicht voor de organisatie. Een gezamenlijke aanpak draagt organisatiebreed bij aan het in control zijn en blijven. Bovendien geeft dit een impuls aan het behalen van de in hoofdstuk 1 beschreven ambities. Gegevensbescherming zal nauwer moeten aansluiten op de P&C-cyclus. Dit betekent onder meer dat:

- de onderwerpen privacy en informatiebeveiliging een rol krijgen in de door de organisatie gehanteerde GRC-tool;[10]
- de doelen uit het gemeentelijke informatiebeveiligingsplan en het gemeentelijke privacyplan opgenomen worden in een paragraaf van de begroting;
- verantwoording over de doelen plaatsvindt in de jaarstukken en, indien noodzakelijk, in de bestuursrapportages.

<u>Overlegstructuren</u>
De gemeente kent verschillende rollen die betrokken zijn bij de onderwerpen privacy en informatiebeveiliging. In het kader van signaleren, zelfleren en verbeteren is het noodzakelijk dat de betreffende functionarissen elkaar periodiek bijpraten over ontwikkelingen op het gebied van informatiebeveiliging en privacy.

Ambtelijk overleg
Er is een integrale overlegstructuur ingericht waarin onderlinge afstemming plaatsvindt tussen ICT-beheer, informatisering, informatiebeveiliging en privacy. In de huidige situatie is dit het driewekelijkse Fg-overleg.

Ook sluiten de privacy officer en de CISO aan bij het Control Kamer Overleg (CKO) dat eens per kwartaal plaatsvindt. Het CKO heeft tot doel om alle disciplines waar compliance, control en risicomanagement een rol spelen, kennis en ervaringen met elkaar te laten uitwisselen om zo van elkaar te kunnen leren en, daar waar mogelijk, gezamenlijk op te trekken.

10) De applicatie die wordt gebruikt voor het beheren van de algehele governance van de organisatie, het beheer van risico's en het naleven van regelgeving.

Daarnaast hebben de privacy officer en de CISO periodiek een overlegmoment met elke individuele teammanager. Dit overleg heeft tot doel elkaar wederzijds op de hoogte te houden van nieuwe ontwikkelen, ondersteuning te bieden aan de teammanager bij zijn taken en om actuele, team-specifieke cases te bespreken.

Crisisoverleg
In tijden van crises en bij grote incidenten is het noodzakelijk dat er op adequate wijze wordt gereageerd. Daarvoor is een goed georganiseerd crisisteam noodzakelijk. De samenstelling van het crisisteam, de rol- en taakverdeling binnen het team en de belangrijkste acties gedurende een crisis, staan beschreven in een crisisprotocol. Het crisisteam zal de stappen uit het crisisprotocol periodiek moeten oefenen om zo de knelpunten in het protocol te ontdekken.

Portefeuillehoudersoverleg
Met de bestuurlijk verantwoordelijk portefeuillehouder vindt periodiek een overleg plaats. Zo blijft de bestuurder betrokken bij privacy en informatiebeveiliging en kan deze de bestuurlijke bijdrage leveren in lopende zaken. Met de portefeuillehouder wordt besproken wanneer en op welke wijze de raad betrokken wordt.

Vastgesteld op: 11 januari 2022 door het college van burgemeester en wethouders van gemeente Wageningen.

BIJLAGE A Privacy principes

De privacyprincipes volgen uit de thema's die de privacywetgeving heeft neergelegd voor de bescherming van persoonsgegevens. De AVG geeft in artikel 5 deze principes duidelijk aan. Deze principes worden ook toegepast door de gemeente.

De gemeente verwerkt persoonsgegevens legitiem ('rechtmatig, behoorlijk, transparant')
Gemeente Wageningen verwerkt alleen persoonsgegevens wanneer dat legitiem is. Legitiem gebruik van persoonsgegevens voldoet aan 3 voorwaarden, namelijk:

- Rechtmatigheid: er is een wettelijke basis voor de verwerking, die past bij het doel van de verwerking. Dit heet 'grondslag voor de verwerking' en is de onderbouwing waarom de gemeente vindt dat zij bepaalde persoonsgegevens mag verwerken.
  Er zijn 6 grondslagen, waarvan de belangrijkste zijn: 'wettelijke verplichting', 'algemeen belang' en 'gerechtvaardigd belang van de gemeente Wageningen'.
- Behoorlijk: de persoonsgegevens worden op een manier verwerkt die past bij het verwerkingsdoel. De inbreuk op de persoonlijke levenssfeer van individuen moet in verhouding staan tot de verwerkingsdoeleinden én de doeleinden moeten niet op een andere, voor individuen minder nadelige wijze, bereikt kunnen worden. De wetgever wil hiermee voorkomen dat voor kleine verwerkingsdoelen juist grote inbreuken op de privacy van individuen maken.
- Transparant: de betrokkene weet welke persoonsgegevens over hem verzameld worden en voor welk doel. Daarnaast wordt hem uitgelegd welke privacyrechten hij heeft en hoe hij die rechten bij de gemeente kan uitoefenen. Er zijn een zevental privacyrechten. De belangrijkste zijn: recht op inzage, recht op wijziging, recht op verwijdering, recht op verzet (tegen de verwerking).

Gemeente Wageningen verwerkt alleen persoonsgegevens met een duidelijk doel ('doelbinding')
Gemeente Wageningen verzamelt en gebruikt alleen persoonsgegevens voor vastomlijnde en beschreven doelen. Als persoonsgegevens worden hergebruikt voor een nieuw of ander werkproces, dan moet het doel hiervan liggen in het verlengde van het doel waarvoor de gegevens oorspronkelijk verzameld zijn ('verenigbaar').

Gemeente Wageningen verwerkt alleen noodzakelijke persoonsgegevens ('dataminimalisatie')
Gemeente Wageningen gebruikt alleen de persoonsgegevens die van belang zijn voor het doel van de verwerking. De gemeente wil voorkomen dat medewerkers persoonsgegevens verzamelen, die 'handig zijn' of 'straks wellicht nodig zijn'. Vaak worden die gegevens niet gebruikt of is op het moment van gebruik niet meer actueel.

Gemeente Wageningen houdt persoonsgegevens actueel ('juistheid')
Gemeente Wageningen zorgt ervoor dat persoonsgegevens die zij verzamelt gecontroleerd worden, zodat ze actueel zijn. Wanneer gegevens worden bewaard, zorgt de gemeente ervoor dat persoonsgegevens actueel blijven. Dit vraagt om onderhoud. Als dat niet mogelijk is, worden de gegevens vernietigd.

Gemeente Wageningen bewaart alleen noodzakelijke persoonsgegevens ('opslagbeperking')
Gemeente Wageningen hanteert voor alle verwerkingen bewaartermijnen. Persoonsgegevens die niet meer nodig zijn, worden verwijderd. Dit betekent dat verwijdering plaatsvindt zodra de wettelijke bewaartermijn is verlopen of - bij afwezigheid van een wettelijke bewaartermijn - nadat het doel van de verwerking is bereikt. Praktisch zal dat vaak betekenen dat slechts een deel van het dossier wordt geschoond, omdat bepaalde gegevens nog langer nodig zijn.

Gemeente Wageningen beschermt haar persoonsgegevens (' beveiliging','privacy by default' en 'privacy by design')
Gemeente Wageningen beschermt haar persoonsgegevens. Dit doet zij met behulp van de principes van informatiebeveiliging en door gebruik te maken van:

- Technische maatregelen, bijvoorbeeld door de toegang tot informatiesystemen te beperken en te scannen op inbreuken (virussen/malware) en technische kwetsbaarheden.
- Organisatorische maatregelen, bijvoorbeeld met beleid, procedures, opleidingen en het bevorderen van de bewustwording van de medewerkers.

Gemeente Wageningen verwacht van alle medewerkers een actieve bijdrage aan beveiliging, door bewust en veilig om te gaan met (persoons)gegevens en door incidenten en verbeterpunten te melden. En daarmee bij te dragen aan een hoog niveau van beveiliging en continue verbetering.

Als gemeente Wageningen zelf applicaties of websites ontwerpt en beheert, zorgt zij ervoor dat de standaard instellingen zo privacyvriendelijk mogelijk staan ingesteld. Door het toepassen van dit principe van 'privacy by default' voorkomt de gemeente dat zij haar gebruikers onbewust meer persoonsinformatie laat prijsgeven dan nodig is voor het gebruik van de functionaliteit. Desgewenst kan de gebruiker zijn instellingen bijstellen en meer van zijn privacy vrijgegeven als hij dat wenst.

Als gemeente Wageningen een nieuw product of dienst ontwikkelt, dan houdt zij vanaf het begin van de ontwerpfase rekening met privacy. Dit principe heet 'privacy by design' en heeft tot doel de bescherming van persoonsgegevens te optimaliseren. Een data protection impact assessment (DPIA) is een geschikt instrument om in te zetten in de ontwerpfase van een nieuw proces. Een goed uitgevoerde DPIA geeft inzicht in de risico's die de verwerking oplevert voor de betrokkenen en in de maatregelen die genomen moeten worden om de risico's af te dekken.

Gemeente Wageningen heeft haar privacyprocessen ingericht en aantoonbaar op orde
De AVG verplicht de gemeente om een aantal processen voor privacy in te richten en wel zodanig dat zij hierover verantwoording kan afleggen aan de (interne) toezichthouder. De gemeente heeft voor AVG een verantwoordingsplicht. Daarom heeft de gemeente deze processen ingericht en wordt op de uitvoering intern toezicht gehouden door de Functionaris Gegevensbescherming.