GEMEENTE waadhoeke

GEMEENTEBLAD

Officiële uitgave van de gemeente Waadhoeke

Nr. 291702

18 juni

2026

Strategisch informatiebeveiligings- en privacybeleid

1. Inleiding

De (digitale) wereld ontwikkelt zich in hoog tempo en zal dit de komende jaren ook blijven doen. Denk bij deze ontwikkelingen aan verdere digitalisering, de inzet van artificial intelligence (AI) en intensiever gebruik van (persoons)gegevens (datagedreven werken). Dit biedt volop kansen om efficiënter te werken en onze dienstverlening te verbeteren. Tegelijkertijd zien we een sterke toename in de afhankelijkheid van systemen en de complexiteit van digitale dreigingen. Zoals gerichte ransomware-aanvallen, datalekken en geavanceerde vormen van cybercriminaliteit. Ook ontwikkelingen op het gebied van wet- en regelgeving, zoals de implementatie van de Cyberbeveiligingswet (NIS2-richtlijn) en actievere inzet van toezichtsmaatregelen door de Autoriteit Persoonsgegevens (AP) onderstrepen het belang van een robuuste informatiebeveiliging en bescherming van persoonsgegevens.

Deze ontwikkelingen vormen de aanleiding voor het opstellen van ons strategisch informatiebeveiligings- en privacybeleid (hierna: strategisch beleid). Informatiebeveiliging en privacy zijn niet langer uitsluitend technische of juridische vraagstukken, maar raken het fundament van het vertrouwen dat inwoners, medewerkers, ondernemers en (samenwerkings)partners (betrokkenen) in ons hebben. Met dit strategisch beleid zetten we een duidelijke koers uit voor de komende vier jaar: van bewustwording tot borging, van reactief naar proactief, met informatiebeveiliging en privacy (IB&P) als integraal onderdeel van ons handelen. Het biedt ruimte voor innovatie en draagt bij aan een transparante en toekomstbestendige organisatie.

1.1 Doel

Het doel van het strategisch beleid is om de ambities en doelen die we nastreven op het gebied van informatiebeveiliging en privacy een plek te geven. Onze wettelijke verplichtingen vormen het kader waarbinnen we bewegen, het zijn de vereisten waaraan we minimaal moeten voldoen. Dat weerhoudt ons er echter niet van om te kijken naar wat we nog meer willen en kunnen doen.

Het strategisch beleid is richtinggevend en kaderstellend en wordt aangevuld met onderwerpspecifieke beleidsdocumenten voor informatiebeveiliging en privacy op tactisch niveau en werkinstructies op operationeel niveau. Het beleid biedt ondersteuning aan het bestuur, het management en de organisatie bij de sturing en beheersing van informatiebeveiliging en privacy. Hiermee zet gemeente Waadhoeke een volgende stap in het versterken van de beveiliging van informatie en de bescherming van persoonsgegevens.

1.2 Scope

In het strategisch beleid staan de strategische keuzes op het gebied van informatiebeveiliging en privacy (IB&P) voor de komende vier jaar. Het vervangt het eerder door het college vastgestelde informatiebeveiligingsbeleid en privacybeleid.

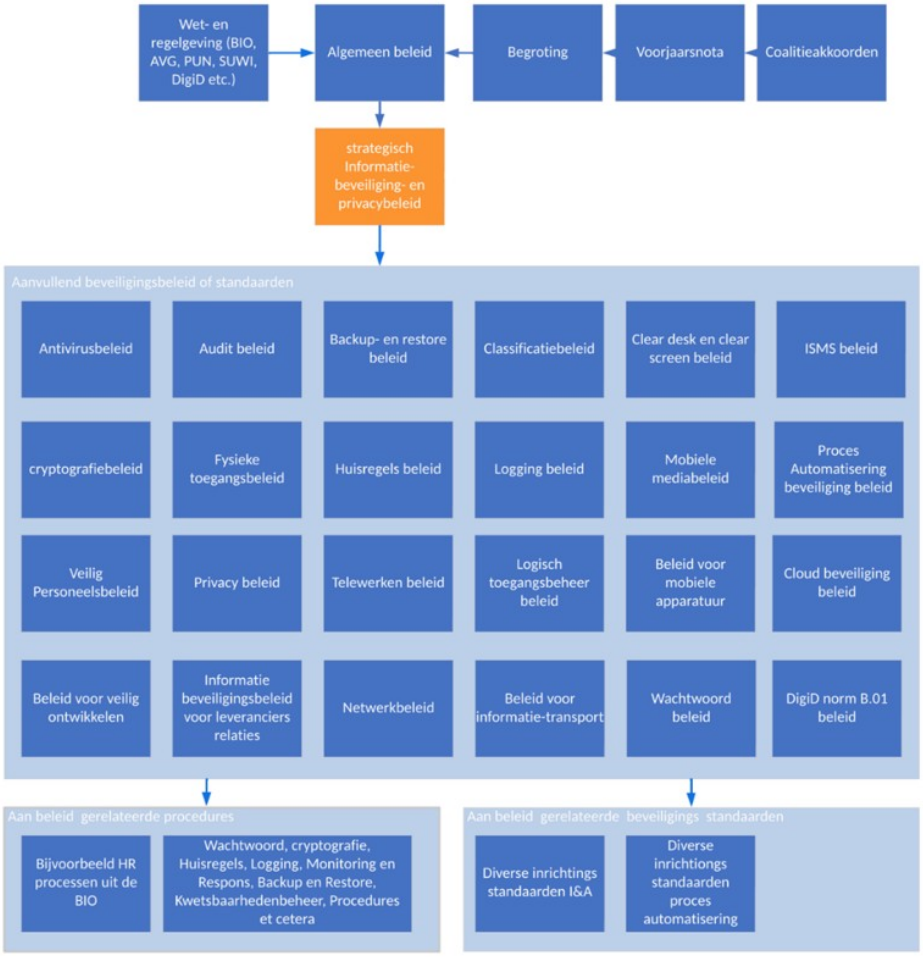
De scope van dit strategisch beleid omvat alle gemeentelijke processen, onderliggende informatiesystemen, procesautomatisering, informatie en (persoons)gegevens van onze gemeente en externe partijen (bijvoorbeeld politie), het gebruik daarvan door medewerkers en (keten)partners in de meest brede zin van het woord, ongeacht locatie, tijdstip en gebruikte apparatuur. Het borgt daarmee de informatievoorziening gedurende de hele levenscyclus, ongeacht de toegepaste technologie en ongeacht het karakter van de informatie. Het beperkt zich niet alleen tot de ICT.

Het beleid biedt een algemene basis en dekt tevens aanvullende beveiligingseisen uit wetgeving af zoals de Algemene Verordening Gegevensbescherming (AVG), Uitvoeringswet AVG (UAVG), Wet politiegegevens (Wpg), Wet basisregistratie personen (Wet BRP), Regeling beheer en toezicht BRP en reis- en waardedocumenten (PNIK), Paspoortuitvoeringsregeling Nederland 2001 (PUN), DigiD en Wet structuur uitvoeringsorganisatie werk en inkomen (SUWI). Voor bepaalde kerntaken gelden op grond van deze wet- en regelgeving ook nog enkele specifieke (aanvullende) beveiligingseisen (bijvoorbeeld SUWI en gemeentelijke basisregistraties) en DigiD met norm B.01 eisen. Deze worden in aanvullende beleidsdocumenten 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.

1.3 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.

In dit beleid beschrijven we op strategisch niveau onze koers als het gaat om informatiebeveiliging en privacy. Dit beleid zal worden vertaald in aanvullend beleid en tactische en operationele richtlijnen en maatregelen. De daaruit voortkomende werkzaamheden worden uitgewerkt in het jaarlijks te schrijven informatiebeveiligingsplan en privacyplan. Onderstaande afbeelding geeft een voorbeeld van de plaats die het strategisch beleid in de organisatie in kan nemen.



Figuur 1 Voorbeeld van de positionering van het Strategisch Informatiebeveiligings- en privacybeleid ten opzichte van overige beleidsdocumenten (kapstok)

1.4 Looptijd en actualisatie van het strategisch beleid

Het strategisch beleid vormt het formele kader voor de inrichting, uitvoering en verantwoording van zowel informatiebeveiliging als privacy en gegevensbescherming binnen de organisatie en kent geen afgebakende looptijd.

Het strategisch beleid wordt jaarlijks geëvalueerd en tussentijds geactualiseerd als daar aanleiding toe is. Aanleidingen voor actualisatie zijn onder meer:

- Wijzigingen in wet- en regelgeving, zoals de inwerkingtreding van de Cyberbeveiligingswet (Cbw), aanpassingen in de Baseline Informatiebeveiliging Overheid (BIO2), relevante sectorale privacy-regels of andere nieuwe privacywetgeving naast de reeds geldende AVG.
- Nieuwe of gewijzigde dreigingen en risico's, bijvoorbeeld uit het jaarlijks dreigingsbeeld van de Informatiebeveiligingsdienst (IBD), interne en externe risicoanalyses of Data Protection Impact Assessments (DPIA's).
- Significante technologische ontwikkelingen, zoals de introductie van nieuwe systemen, cloudoplossingen of operationele technologie of het gebruik van AI en algoritmes.

- Bevindingen uit audits, self-assessments, incidentanalyses of toezicht door de Rijksinspectie Digitale Infrastructuur (RDI) en de AP.
- Wijzigingen in de organisatie, processen of samenwerkingsverbanden die impact hebben op de informatievoorziening of de verwerking van persoonsgegevens.

Gemeente Waadhoeke waarborgt de actualiteit van het beleid door:
- Jaarlijkse beoordeling van het beleid in aansluiting op de planning & control-cyclus en relevante externe ontwikkelingen.
- Structurele monitoring van wet- en regelgeving, dreigingsbeelden, technologische ontwikkelingen en privacy-ontwikkelingen.
- Direct initiëren van een actualisatieproces bij geconstateerde afwijkingen, nieuwe verplichtingen of relevante incidenten op het gebied van informatiebeveiliging of privacy.
- Integratie van privacyaspecten in alle fasen van beleid en uitvoering, waarbij expliciet aandacht is voor de zes beginselen van de AVG: rechtmatigheid, doelbinding, dataminimalisatie, juistheid, opslagbeperking en vertrouwelijkheid/integriteit.

1.5 Leeswijzer
In hoofdstuk 2 van het strategisch beleid gaan we dieper in op informatiebeveiliging en privacy. We staan stil bij wat er onder deze thema's wordt verstaan en hoe ze zich tot elkaar verhouden. Ook bespreken we in hoofdstuk 2 de relevante ontwikkelingen die invloed hebben op informatiebeveiliging en privacy binnen gemeente Waadhoeke.

In het derde hoofdstuk staan we stil bij de visie en ambitie van gemeente Waadhoeke op het gebied van informatiebeveiliging en privacy. Deze visie en ambitie werken we uit in concrete doelstellingen waar we aan gaan werken de komende jaren.

In hoofdstuk 4 werken we de taken en verantwoordelijkheden op het gebied van informatiebeveiliging en privacy uit. Dit doen we enerzijds specifiek voor de Chief Information Security Officer (CISO), Functionaris Gegevensbescherming (FG) en Privacy Security Officer (PSO) en anderzijds voor de organisatie, het management, directie en het bestuur in het algemeen.

2. Informatiebeveiliging en privacy

Informatiebeveiliging en privacy zijn onlosmakelijk met elkaar verbonden. Beide onderwerpen zijn geen eenmalig project, maar een cyclisch en risicogestuurd proces dat continu wordt geëvalueerd en geactualiseerd op basis van nieuwe dreigingen, technologische ontwikkelingen en wijzigingen in wet- en regelgeving.

2.1 Informatiebeveiliging
Gemeente Waadhoeke borgt de betrouwbaarheid van haar informatievoorziening door informatiebeveiliging structureel, aantoonbaar en integraal te organiseren. Dit betekent dat wij continu een samenhangend pakket van technische, organisatorische en procesmatige maatregelen nemen en onderhouden. Hiermee beschermen wij de beschikbaarheid, integriteit en vertrouwelijkheid van alle informatie die binnen gemeentelijke organisatie wordt verwerkt – van persoonsgegevens en beleidsinformatie tot videobeelden en kennis van medewerkers.

Informatiebeveiliging omvat alle vormen van informatie: analoog en digitaal, tekst, beeld, geluid, geheugen en kennis. Ook alle informatiedragers vallen hieronder, van papier en elektronische bestanden tot foto's, films, cd's/dvd's en beeldschermen. Informatiebeveiliging geldt voor alle informatieverwerkende systemen, zoals software, databases, hardware en bedrijfsmiddelen. Wij richten ons zowel op de processen waarin deze informatie wordt gebruikt als op de mensen die ermee werken.

Het strategische beleid is van toepassing op iedereen die gebruikmaakt van gemeentelijke informatiesystemen: Het college, de directie, managers, medewerkers, de gemeenteraad (inclusief (schaduw)fracties), de griffie, externe relaties, samenwerkingspartners en overige gebruikers, ongeacht locatie, tijdstip of gebruikte systemen.

De omvang en complexiteit van (digitale) dreigingen voor gemeenten nemen jaarlijks toe. Ransomware, datalekken, uitval van processen door incidenten en verstoringen bij leveranciers vormen de grootste risico's. Daarom zijn basismaatregelen zoals multifactorauthenticatie, netwerksegmentatie, back-ups, monitoring en bewustwording verplicht en structureel geborgd. Leveranciersmanagement is aangescherpt met expliciete eisen aan informatiebeveiliging en controle op naleving. Training en bewustwording van bestuur, directie, management en medewerkers zijn vast onderdeel van het beleid en worden periodiek getoetst.

2.1.1 Wettelijk en normatief kader

Gemeente Waadhoeke bereidt zich voor op de inwerkingtreding van de Nederlandse Cbw, waarin de Europese NIS2-richtlijn wordt omgezet in nationale wetgeving. De NIS2-richtlijn trad op 16 januari 2023 in werking in de lidstaten om de digitalisering van onze samenleving veiliger te maken. Lidstaten kregen een termijn van 21 maanden om de regels te vertalen naar nationale wetgeving; formeel had Nederland de Cbw daarom op 17 oktober 2024 in werking moeten laten treden. In de praktijk verloopt de implementatie echter vertraagd, en streeft de regering ernaar om de wet in het tweede kwartaal van 2026 definitief van kracht te laten worden.

Binnen onze gemeente speelt niet alleen traditionele ICT een rol, maar ook Operationele Technologie (OT). OT omvat digitale systemen die fysieke infrastructuur aansturen, zoals verkeerslichten, rioolgemalen en bruggen.
De BIO2 is van toepassing op de informatiebeveiliging van alle gemeentelijke netwerk- en informatiesystemen en alle typen omgevingen. Voor de bescherming van de OT-omgevingen hanteren we de Cybersecurity Implementatie Richtlijn (CSIR). Op die manier waarborgt ons beleid zowel de digitale als de fysieke continuïteit van gemeentelijke processen.

Het college van burgemeester en wethouders is expliciet verantwoordelijk voor het treffen van passende en evenredige technische, organisatorische en operationele maatregelen, afgestemd op de relevante risico's.

Informatiebeveiliging is geen keuze, maar een wettelijke plicht. De Baseline Informatiebeveiliging Overheid 2 (BIO2) is het verplichte normenkader voor alle overheidsorganisaties en is gebaseerd op de internationale normen NEN-EN-ISO/IEC 27001 en 27002. De Cbw maakt de toepassing van de BIO2 wettelijk verplicht.

Gemeente Waadhoeke richt een managementsysteem voor informatiebeveiliging (ISMS) in en borgt deze. In het ISMS worden risicomanagement, maatregelen en verantwoording structureel vastgelegd. Risicoanalyses worden systematisch uitgevoerd en vastgelegd en de opzet, het bestaan en de werking van maatregelen zijn aantoonbaar. Afwijkingen van verplichte maatregelen worden gemotiveerd vastgelegd in de Verklaring van Toepasselijkheid (VvT). De effectiviteit van het strategisch beleid wordt periodiek getoetst via interne en externe audits, self-assessments en rapportages. De reikwijdte van het ISMS en de VvT worden gepubliceerd, en jaarlijks wordt gerapporteerd over de status van informatiebeveiliging.

Het college van B&W is verplicht om aantoonbaar voldoende kennis en vaardigheden te hebben, onder meer door periodieke training. Zij zijn verantwoordelijk voor het tijdig melden van ernstige digitale incidenten bij de toezichthouder en voor het borgen van de continuïteit van de dienstverlening bij verstoringen. De gemeenteraad houdt toezicht op de naleving, terwijl de Rijksinspectie Digitale Infrastructuur (RDI) toezicht houdt op de gehele overheid. Overtredingen van de zorgplicht en meldplicht kunnen leiden tot bestuurlijke en persoonlijke boetes.

We volgen de verplichte overheidsmaatregelen uit de BIO2 altijd, tenzij deze aantoonbaar niet van toepassing zijn. Afwijkingen onderbouwen we en leggen we vast in de VvT. Informatiebeveiliging is integraal onderdeel van de bedrijfscontinuïteit en crisisbeheersing. Transparantie en verantwoording zijn leidend: inwoners, bedrijven en andere belanghebbenden moeten kunnen vertrouwen op een zorgvuldige en veilige omgang met hun gegevens.

De 10 bestuurlijke principes voor informatiebeveiliging

De 10 bestuurlijke principes voor informatiebeveiliging[1] vormen een aanvulling op de BIO2. Ze geven richting aan het handelen van bestuurders en leggen vast welke waarden en uitgangspunten het bestuur zichzelf oplegt. Deze principes zijn bedoeld om informatiebeveiliging stevig te verankeren in het bestuurlijk handelen en ondersteunen bestuurders bij het nemen van verantwoordelijkheid en het uitvoeren van effectief risicomanagement binnen de gemeentelijke organisatie. Incidenten op het gebied van informatiebeveiliging kunnen directe gevolgen hebben voor inwoners, ondernemers en (samenwerkings)partners van de gemeente. Daarom hoort het onderwerp structureel op de bestuurlijke agenda en vraagt het om actieve betrokkenheid en sturing vanuit het bestuur.

1. **Bestuurders stimuleren een veilige cultuur.**

1) https://vng.nl/files/vng/de-10-bestuurlijke-principes-voor_20190109.pdf

Zij geven het goede voorbeeld, spreken elkaar aan en creëren een omgeving waarin veiligheid vanzelfsprekend is.
2. **Informatiebeveiliging is een gezamenlijke verantwoordelijkheid.**
   Iedereen binnen de organisatie, van bestuur tot medewerker, draagt bij aan een veilige informatievoorziening
3. **Informatiebeveiliging is onlosmakelijk verbonden met risicomanagement.**
   Het bestuur zorgt ervoor dat risico's op het gebied van informatiebeveiliging systematisch worden herkend, beoordeeld en beheerst
4. **Risicomanagement is een integraal onderdeel van besluitvorming.**
   Bestuurlijke keuzes worden altijd genomen met expliciete aandacht voor digitale risico's en de impact op de organisatie en haar omgeving
5. **Informatiebeveiliging vraagt aandacht in alle samenwerkingsverbanden.**
   Ook in de keten en bij externe partners worden heldere eisen gesteld en afspraken gemaakt over digitale veiligheid
6. **Informatiebeveiliging is een continu proces.**
   Het bestuur borgt dat informatiebeveiliging cyclisch wordt geëvalueerd en structureel wordt verbeterd
7. **Informatiebeveiliging vereist structurele investeringen.**
   Het bestuur reserveert voldoende middelen en capaciteit om het gewenste beveiligingsniveau te realiseren en te behouden
8. **Onzekerheid en onvoorziene risico's worden meegenomen in de afwegingen.**
   Het bestuur accepteert dat niet alle risico's volledig uit te sluiten zijn en houdt rekening met onzekerheden in beleid en uitvoering
9. **Leren en verbeteren staan centraal.**
   Incidenten, audits en evaluaties worden actief gebruikt om de organisatie en processen continu te verbeteren
10. **Het bestuur houdt toezicht en stuurt bij waar nodig.**
    Door periodiek te controleren en te evalueren, blijft informatiebeveiliging actueel en effectief.

2.2 Privacy & gegevensbescherming
Gemeente Waadhoeke werkt met persoonsgegevens van inwoners, ondernemers, medewerkers en (keten)partners. Deze gegevens verzamelen we voor het goed kunnen uitvoeren van onze gemeentelijke en wettelijke taken. Denk hierbij aan taken in het sociaal domein, openbare orde en veiligheid of voor burgerzaken. Om deze taken goed uit te kunnen voeren zijn persoonsgegevens noodzakelijk.

De bescherming van persoonsgegevens – kortweg vaak privacy genoemd – is een breed begrip dat uit meerdere aspecten bestaat. 'Bescherming' omvat in dit geval meer dan alleen beveiliging van persoonsgegevens. Ook het zorgen voor juiste, doel- en rechtmatige verwerkingen van persoonsgegevens en het bewaren van deze gegevens behoort tot het begrip 'bescherming'. Het is een samenspel van verschillende vakgebieden dat zich organisatiebreed afspeelt.

In de AVG zijn de beginselen opgenomen waaraan deze bescherming moet voldoen.

Basisbeginselen voor de verwerking van persoonsgegevens op grond van de AVG
1. Er is altijd een wettelijke grondslag.
2. Er is een duidelijk doel voor het verwerken van persoonsgegevens vastgesteld.
3. Er worden niet meer persoonsgegevens dan nodig verwerkt.
4. Er wordt met juiste en actuele gegevens gewerkt.
5. De gegevens worden niet langer bewaard dan noodzakelijk.
6. Er worden technische en organisatorische maatregelen genomen om de persoonsgegevens te beschermen tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging.

Bij de omgang met persoonsgegevens draagt gemeente Waadhoeke een grote verantwoordelijkheid. Privacy is een complex en noodzakelijk vraagstuk. Dit komt mede door de toenemende digitalisering van de samenleving, de decentralisatie van overheidstaken, gegevensuitwisseling met (keten)partners, technologische ontwikkelingen en veranderende wetgeving. Het is een strategische – en daarmee ook organisatiebrede – opgave die raakt aan beleid, dienstverlening, informatievoorziening en -huishouding en uitvoering. Omdat de AVG slechts op hoofdlijnen kadert en geen operationele invulling biedt voor specifieke verwerkingen, vraagt het borgen van privacy om een integrale en multidisciplinaire benadering. Dit betekent dat juridische, organisatorische en technologische expertise samen moeten komen en dat privacyvraagstukken op strategisch, tactisch én operationeel niveau spelen. De verwevenheid met andere vakgebieden maakt uitwisseling van kennis en ervaringen met diverse disciplines van groot belang om tot zorgvuldige en toekomstbestendige oplossingen voor privacyvraagstukken te komen.

Privacy verdient continu aandacht binnen gemeente Waadhoeke. Inwoners, medewerkers, ondernemers en (samenwerkings)partners moeten erop kunnen vertrouwen dat wij als gemeente zorgvuldig en veilig met hun persoonsgegevens omgaan.

2.2.1 Wettelijk en normatief kader

Voor de bescherming van persoonsgegevens houdt gemeente Waadhoeke zich aan verschillende wet- en regelgeving. Dit gaat om Europese verordeningen, nationale wetgeving en sectorspecifieke wetten. Daarnaast hebben verschillende ontwikkelingen invloed op hoe we omgaan met persoonsgegevens. Hieronder zetten we de belangrijkste uiteen.

De Algemene Verordening Gegevensbescherming
Op 25 mei 2018 trad de AVG in werking. De AVG is een Europese Verordening die rechtstreekse werking heeft. Het hoofddoel van de AVG is de bescherming van persoonsgegevens van natuurlijke personen en het faciliteren van het vrije verkeer van die gegevens binnen de Europese Unie. De AVG versterkt de privacyrechten van individuen en legt tegelijkertijd meer verantwoordelijkheden bij organisaties die persoonsgegevens verwerken.

De belangrijkste doelen en aspecten van de AVG zijn:

- **Bescherming van privacy**
  De AVG zorgt ervoor dat mensen meer controle hebben over hun persoonsgegevens en dat deze op een veilige en rechtmatige manier worden verwerkt.
- **Harmonisatie van regels**
  De AVG zorgt voor uniforme regels voor de verwerking van persoonsgegevens in alle EU-lidstaten, wat het makkelijker maakt voor bedrijven die in meerdere landen actief zijn.
- **Rechten van betrokkenen**
  De AVG geeft mensen diverse rechten, zoals het recht op inzage, recht op correctie, recht op vergetelheid (wissen van gegevens) en recht op dataportabiliteit (overdracht van gegevens).
- **Verantwoordelijkheden voor organisaties**
  Organisaties moeten aantonen dat ze de AVG naleven, bijvoorbeeld door een register van verwerkingsactiviteiten bij te houden, een DPIA uit te voeren bij risicovolle verwerkingen en maatregelen te nemen voor 'privacy by design' en 'privacy by default'.
- **Toezicht en handhaving**
  De AVG voorziet in een onafhankelijke toezichthouder, de AP in Nederland, die toezicht houdt op de naleving van de AVG en boetes kan opleggen bij overtredingen. In het verlengde daarvan verplicht de AVG overheidsinstanties om een interne, onafhankelijke toezichthouder, de Functionaris Gegevensbescherming, te benoemen.
- **Moderne technologie**
  De AVG is ontworpen om rekening te houden met de ontwikkelingen in de digitale wereld en de toegenomen verzameling en verwerking van persoonsgegevens.

Uitvoeringswet Algemene Verordening Gegevensbescherming
De AVG geeft ruimte aan de lidstaten om bepaalde zaken verder uit te werken in nationale wetgeving. In Nederland is daar vorm aan gegeven middels de UAVG. De UAVG bevat onder andere:

- **Benoeming van de AP als toezichthoudende instantie**
  De AP houdt toezicht op de naleving van de AVG en UAVG en andere gerelateerde privacy wet- en regelgeving.
- **Uitzonderingen en specifieke bepalingen**
  De UAVG voorziet op bepaalde punten, zoals bij de verwerking van persoonsgegevens in de zorg, of voor specifieke sectoren, in regels die een aanvulling vormen op de AVG.
- **Regels voor de verwerking van strafrechtelijke gegevens**
  De UAVG bevat specifieke bepalingen voor de verwerking van persoonsgegevens die verband houden met strafrechtelijke veroordelingen en strafbare feiten.
- **Verantwoordelijkheden en plichten van organisaties**
  De UAVG verduidelijkt de verantwoordelijkheden van organisaties bij het verwerken van persoonsgegevens.
- **Rechten van betrokkenen**
  De UAVG bevestigt de rechten van betrokkenen, zoals het recht op informatie, rectificatie en verwijdering van persoonsgegevens.

De Wet politiegegevens
Bijzondere Opsporingsambtenaren (BOA) kunnen meerdere taken en bevoegdheden hebben waarbij rekening moet worden gehouden met verschillende wet- en regelgeving. In het kader van de verwerking van persoonsgegevens door BOA kunnen twee regimes van toepassing zijn: de AVG en/of de Wpg. In

de Wpg en het bijbehorende Besluit politiegegevens (Bpg) staat dat de Wpg van toepassing is op gegevensverwerkingen door BOA voor de uitvoering van hun opsporingstaak. Het gaat om de opsporing van strafbare feiten die in een akte van opsporingsbevoegdheid of in een aanwijzing zijn opgelegd aan de BOA. Gemeente Waadhoeke heeft BOA in dienst die persoonsgegevens verwerken die onder de AVG en onder de Wpg vallen.

De FG die is benoemd om toezicht te houden op de naleving van de AVG, is ook met de taak belast om toezicht te houden op de verwerking van politiegegevens als daar binnen de organisatie geen andere FG voor is aangesteld. Binnen gemeente Waadhoeke is er één FG aangesteld die de toezichthoudende taken op grond van zowel de AVG als Wpg uitvoert.

2.3 De relatie tussen informatiebeveiliging en privacy
Informatiebeveiliging en privacy worden in de praktijk vaak in één adem genoemd. Niet zonder reden, want beide domeinen raken aan het zorgvuldig omgaan met (persoons)gegevens. Toch zijn het wezenlijk verschillende vakgebieden, elk met een eigen scope, systematiek en juridische grondslag.

Informatiebeveiliging richt zich op het beschermen van alle informatie die van waarde is voor de organisatie. Dat gaat nadrukkelijk verder dan alleen persoonsgegevens. Denk aan beleidsstukken, financiële gegevens, ruimtelijke plannen, maar ook aan de beschikbaarheid van systemen en de continuïteit van de dienstverlening. De kernprincipes van informatiebeveiliging – beschikbaarheid, integriteit en vertrouwelijkheid – vormen het fundament onder dit domein. De focus ligt daarbij op risicoanalyse, beheersmaatregelen en het aantoonbaar maken van weerbaarheid tegen verstoringen, incidenten en dreigingen.

Privacy, of meer specifiek gegevensbescherming, zoomt in op de verwerking van persoonsgegevens. De AVG stelt hier strikte eisen aan, die verder gaan dan technische beveiliging. Aspecten als rechtmatigheid, transparantie, doelbinding en dataminimalisatie zijn hier minstens net zo belangrijk. Informatiebeveiliging is primair risicogestuurd en richt zich op het beschermen van het organisatiebelang. De aanpak is gebaseerd op inschattingen van dreiging en impact, maar houdt ook rekening met wet- en regelgeving.
Privacyregelgeving is primair normatief. De wet bepaalt welke rechten en plichten gelden bij de verwerking van persoonsgegevens. Het richt zich op het beschermen van de belangen van betrokkenen. Ook zonder concreet risico op schade moeten deze normen worden nageleefd.

Toch is er sprake van samenhang. De bescherming van persoonsgegevens vraagt óók om passende beveiligingsmaatregelen. In die zin is informatiebeveiliging een noodzakelijk onderdeel om privacy en gegevensbescherming te kunnen borgen. Vandaar ook de verplichtingen in de AVG om persoonsgegevens te beveiligen (art. 5, 24, 32 en 34 AVG). Anders gezegd, zonder informatiebeveiliging geen privacy, maar privacy vraagt om méér dan beveiliging alleen.

Figuur 2: Relatie tussen informatiebeveiliging en privacy

Samenwerking tussen beide domeinen vraagt om meer dan inhoudelijke afstemming. Het vereist ook een strategische verankering binnen de organisatie. Zowel informatiebeveiliging als privacy en gegevensbescherming raken immers niet alleen specifieke vakafdelingen, maar de gehele bedrijfsvoering. Iedere medewerker werkt met informatie – vaak met persoonsgegevens – en vrijwel elk proces, intern of richting inwoners, is informatiegedreven. Dit maakt de rol van de CISO en FG niet alleen ondersteu-

nend of controlerend, maar ook adviserend op strategisch niveau, richting directie, management en bestuur. De CISO en FG zorgen voor organisatiebrede afstemming en samenhang.

De organisatie, onze inwoners en ondernemers moeten kunnen vertrouwen op stabiele processen, integere systemen en rechtmatige omgang met gegevens. Alleen dan kunnen publieke taken betrouwbaar worden uitgevoerd en behoudt de gemeente haar legitimiteit richting inwoners en ketenpartners. Informatiebeveiliging en privacy zijn daarin geen sluitpost of incidentgedreven thema's, maar randvoorwaardelijk voor continuïteit, publieke verantwoording en toekomstbestendige digitale dienstverlening.

2.4 Ontwikkelingen
Op beide vakgebieden zijn diverse ontwikkelingen van invloed. De verdere digitalisering van de samenleving, de toegenomen complexiteit van publieke taken en de opkomst van nieuwe technologische oplossingen zorgen ervoor dat informatiebeveiliging en privacy steeds nadrukkelijker op de agenda moeten staan.

2.4.1 Implementatie AI Act
De opkomst van (generatieve) AI biedt zowel kansen als bedreigingen voor gemeenten. AI kan worden ingezet om bedrijfsvoering en dienstverlening te helpen. Het kan ook beveiligingsprocessen efficiënter maken, bijvoorbeeld door geavanceerde monitoring en automatische detectie van verdachte activiteiten. Tegelijkertijd maken criminelen gebruik van AI voor nieuwe aanvalsmethoden zoals deepfake-fraude of gerichte phishingcampagnes.

Sinds de invoering van de AVG is het besef gegroeid dat we een grote verantwoordelijkheid hebben voor controle op de wijze waarop persoonsgegevens van inwoners en medewerkers worden verwerkt. Met de opkomst van AI-toepassingen staat deze controle onder druk. Ook, of juist, wanneer de gemeente zelf terughoudend is bij het toepassen van AI. Het gevaar bestaat dat de organisatie niet meebeweegt met de ontwikkelingen en medewerkers ongereguleerd en uit het zicht zelf AI inzetten voor het eigen werk.

AI-modellen functioneren vaak als een black box. Het is onduidelijk hoe zij data verwerken en waar die terechtkomen. De Europese AI Act reguleert het gebruik van AI en eist dat risico's voor mens en maatschappij worden geminimaliseerd. Gemeenten moeten kunnen aantonen dat ze AI op een zorgvuldige en transparante manier inzetten. Ook hierin is samenwerking tussen informatiebeveiliging en privacy een must om schaarse capaciteit, kennis en onderhandelingskracht te bundelen.

2.4.2 Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten
Uit het dreigingsbeeld Informatiebeveiliging 2025-2026 van de Informatiebeveiligingsdienst (IBD) blijkt dat gemeenten voor een onverminderd complex digitaal dreigingslandschap staan. Ransomware, datalekken en uitval van processen door incidenten vormen de grootste bedreigingen. Dit vraagt om een proactieve aanpak om digitale veiligheid te waarborgen en vertrouwen van inwoners en ondernemers te behouden. Dit alles in het licht van financiële en personele krapte.

De digitale dreigingen raken direct aan de continuïteit van gemeentelijke dienstverlening en het vertrouwen van inwoners. Gemeenten kampen bovendien met beperkte capaciteit, kennis en middelen, wat het moeilijk maakt om de digitale veiligheid op peil te houden. In het licht van structurele tekorten, geopolitieke spanningen en technologische afhankelijkheden is een proactieve én collectieve aanpak bepalend.

Het IBD-rapport bevat een heldere bestuurlijke boodschap: risicomanagement is een kerntaak van elke bestuurder, ook digitaal. Nieuwe wet- en regelgeving zoals de Cbw maakt digitale veiligheid bovendien een expliciete bestuurlijke verantwoordelijkheid.

Het rapport biedt gemeenten concrete handvatten om de weerbaarheid van hun organisatie te versterken, waaronder:
- Basismaatregelen zoals multifactorauthenticatie, netwerksegmentatie, monitoring en back-ups;
- Veilig opdrachtgeverschap aan leveranciers, met expliciete afspraken over beveiliging, incidentrespons en dataminimalisatie;
- Collectieve samenwerking tussen gemeenten om kennis, capaciteit en inkoopkracht te bundelen.

2.4.3 Informatie uit incidenten, inbreuken op de beveiliging en datalekken
Een belangrijke bron voor beleidsontwikkeling op het gebied van informatiebeveiliging en privacy is de analyse van incidenten, beveiligingsinbreuken en datalekken. Zowel binnen gemeenten als landelijk ontstaat steeds meer aandacht voor het structureel benutten van deze meldingen als sturingsinformatie.

Incidentregistraties, meldprocessen en evaluaties leveren inzicht op in waar beleid, uitvoering en techniek in de praktijk niet naadloos op elkaar aansluiten.

De IBD wijst in meerdere publicaties op het belang van structurele incidentanalyse, onder andere als input voor risicomanagement, bewustwordingsmaatregelen en beleidsactualisatie. Gemeenten worden daarin gestimuleerd om meldingen niet alleen op te lossen, maar ook te benutten voor verbetering op organisatieniveau.

3. Visie, ambitie en doelstellingen

Voor gemeente Waadhoeke zijn informatiebeveiliging en privacy niet slechts technische randvoorwaarden, maar het fundament onder ons dagelijks handelen als publieke organisatie. Ze zijn onmisbaar voor de manier waarop we besturen, samenwerken en dienstverlenen. Alleen als informatiebeveiliging en privacy integraal verweven zijn in onze processen, cultuur en samenwerking, kunnen we betrouwbaar, nabij en toekomstgericht opereren.

Onze kernwaarden – vertrouwen, klantgericht, betrouwbaar, integer, doel- en resultaatgericht en omgevingsbewust – zijn slechts geloofwaardig als we aantoonbaar zorgvuldig omgaan met informatie en persoonsgegevens. Ook onze bouwstenen zoals nabij besturen, gebiedsgericht werken, integraal managen, lerend organiseren en flexibel en inclusief zijn komen alleen tot hun recht als informatiebeveiliging en privacy structureel zijn ingebed in ons handelen.

Door structureel en aantoonbaar invulling te geven aan onze verantwoordelijkheid, versterken we het vertrouwen van inwoners, ondernemers, medewerkers en (samenwerkings)partners. Zo leggen we de basis voor een organisatie die niet alleen voldoet aan wet- en regelgeving, maar ook recht doet aan haar publieke rol in een steeds meer digitale, complexe samenleving.

3.1 Visie

De visie van gemeente Waadhoeke op informatiebeveiliging en privacy is dat ze:

- **De basis vormen voor vertrouwen**
  Inwoners, ondernemers, medewerkers en (samenwerkings)partners vertrouwen ons hun (persoons)gegevens toe. Zij moeten ervan uit kunnen gaan dat hun gegevens bij gemeente Waadhoeke in goede handen zijn. Een zorgvuldige en betrouwbare verwerking van (persoons)gegevens vormt de basis voor dat vertrouwen.

- **Voorwaardelijk zijn voor een open en transparante, integere en betrouwbare dienstverlening**
  Persoonlijke, toegankelijke en flexibele dienstverlening is alleen mogelijk als informatiebeveiliging en privacy vanaf het eerste contactmoment geborgd zijn. Betrouwbare informatievoorziening is essentieel voor het behalen van resultaten en het leveren van maatwerk. Door bewust om te gaan met informatie en persoonsgegevens ontstaat niet alleen een robuuste en toekomstbestendige informatievoorziening maar werken we ook aan het versterken van onze dienstverlening. We zijn open en transparant over welke (persoons)gegevens we verwerken en zorgen ervoor dat informatie en persoonsgegevens afgeschermd zijn als dat moet en beschikbaar zijn als dat kan. Een open en transparante, integere en betrouwbare informatievoorziening en dienstverlening is noodzakelijk voor het goed functioneren en vormt de basis voor het beschermen van de rechten van onze inwoners, medewerkers, ondernemers en samenwerkingspartners.

- **De motor zijn voor samenwerking en innovatie**
  In een omgeving van gebiedsgericht werken, nabij besturen en ketensamenwerking is veilig en verantwoord delen van informatie en persoonsgegevens cruciaal. Een goede beveiliging van informatie en bescherming van persoonsgegevens maakt het mogelijk om samen te werken, binnen en buiten de organisatie.

3.2 Ambitie

De ambitie van gemeente Waadhoeke voor informatiebeveiliging en privacy is:

- **Informatiebeveiliging en privacy zijn volledig geïntegreerd in alle processen, projecten en samenwerkingen**
  Informatiebeveiliging en privacy zijn geen verantwoordelijkheid van specialisten alleen, maar van iedereen. Eigenaarschap en aanspreekbaarheid liggen laag in de organisatie, in lijn met onze bouwsteen ‘besliskracht laag’. Leidinggevenden geven het goede voorbeeld en ondersteunen medewerkers om verantwoordelijkheid te nemen.

- **Iedereen in de organisatie is zich bewust van zijn of haar verantwoordelijkheid en beschikt over de kennis om deze verantwoordelijkheid op een goede manier te nemen**
  In iedere laag van de organisatie liggen verantwoordelijkheden voor het op een goede manier waarborgen van de beveiliging van informatie en de bescherming van persoonsgegevens. Vanuit de AVG en BIO2 is het college daarin de eindverantwoordelijke. Maar ook de directie en het management spelen een belangrijke rol in het nemen van maatregelen om risico's te beheersen en wet- en regelgeving na te leven. In lijn met de managementfilosofie, waarin staat dat verantwoordelijkheden laag in onze organisatie liggen, is het tot slot aan onze medewerkers om de beveiliging van informatie en de bescherming van persoonsgegevens in de praktijk te brengen.

- **We nemen onze verantwoordelijkheid in de keten en creëren een positieve impact op onze omgeving**
  Met een proactieve houding nemen we deel in de verschillende netwerken waarin we onze bewegen. We delen onze kennis en ervaring maar halen die ook op als het nodig is. Samenwerken maakt ons sterker. Door de lat hoog te leggen en het optimale na te streven, hebben we een positieve invloed op onze omgeving. We vragen van de partijen waar we mee samenwerken om eenzelfde niveau van beveiliging en bescherming na te leven. Dat heeft impact op onze inwoners, maar kan ook impact hebben op anderen die met deze partijen samenwerken.

3.3 Doelstellingen

Om invulling te geven aan onze visie en ambitie, stellen we onszelf de volgende strategische doelstellingen:

- **Bij nieuwe initiatieven of wijzigingen in processen worden informatiebeveiliging en privacy vroegtijdig meegenomen**
  Door informatiebeveiliging en privacy vanaf de start van nieuwe initiatieven of wijzigingen van processen mee te nemen, worden ze een vast onderdeel van ieder traject. Dat versterkt niet alleen het informatiebeveiligings- en privacybewustzijn maar zorgt ook voor een continue versteviging van de beveiliging van informatie en bescherming van persoonsgegevens.

- **We hebben een positieve impact op onze omgeving**
  Onze kritische houding en hoge eisen aan informatiebeveiliging en privacy werken door in de keten en bij leveranciers. Door onze lat hoog te leggen, stimuleren we ook anderen om hun informatiebeveiliging en privacy te verbeteren. Zo dragen we bij aan een veiliger en betrouwbaarder digitaal ecosysteem, niet alleen voor gemeente Waadhoeke maar ook voor onze partners en de samenleving als geheel.

- **We zijn lerend en flexibel**
  Incidenten en fouten zijn aanleiding voor verbetering, niet voor afrekening. We stimuleren een cultuur van openheid, leren en experimenteren. Iedereen — ongeacht functie of positie — draagt bij aan informatiebeveiliging en privacy en wordt daarop aangesproken.

- **We geven ruimte binnen duidelijke kaders**
  We sturen op vertrouwen, ruimte en verantwoordelijkheid, maar altijd binnen heldere normen en wettelijke kaders (BIO2, Cbw, AVG/UAVG, etc.). We bieden ruimte voor maatwerk, innovatie en ontwikkeling, zonder de basisnormen uit het oog te verliezen.

4. Governance

De verantwoordelijkheid voor informatiebeveiliging en privacy komt toe aan iedereen die met (persoons)gegevens werkt. De mate van verantwoordelijkheid verschilt per organisatielaag. In het nemen van deze verantwoordelijkheid wordt de organisatie ondersteund door de Chief Information Security Officer (CISO), de Functionaris Gegevensbescherming (FG) en de Privacy Security Officer (PSO). Zij vormen het informatiebeveiliging- en privacy team (IB&P-team).

In dit hoofdstuk beschrijven we wie waarvoor verantwoordelijk is, hoe de samenwerking is georganiseerd en welke taken en bevoegdheden bij welke functie zijn belegd. Van het college als eindverantwoordelijke tot de individuele medewerker: iedereen heeft een rol in het beschermen van informatie en persoonsgegevens. In bijlage 1 en 2 worden deze rollen, taken en verantwoordelijkheden uitgebreid uitgewerkt. Alleen door de rollen helder te definiëren en consequent na te leven, kunnen we als gemeente Waadhoeke onze ambities waarmaken: persoonlijk, online en dichtbij.

4.1 Taken en verantwoordelijkheden van het IB&P-team

Het IB&P-team van gemeente Waadhoeke vormt de professionele ruggengraat van onze informatiebeveiliging en privacy en gegevensbescherming. Dit team bestaat uit specialisten die vanuit hun expertise

en onafhankelijke positie de organisatie ondersteunen bij het vormgeven van een weerbare en privacybewuste organisatie.

4.1.1 De Chief Information Security Officer

De CISO is binnen gemeente Waadhoeke de strategisch adviseur en coördinator voor informatiebeveiliging. De CISO is onafhankelijk gepositioneerd in de Staf en fungeert als verbindende schakel tussen bestuur, directie, management en het IB&P-team. De CISO rapporteert direct aan de directie en het bestuur, met korte lijnen naar beide directieleden, de burgemeester (portefeuillehouder) en het college van B&W.

Kerntaken en verantwoordelijkheden

- **Strategisch beleid en advisering**
  De CISO ontwikkelt en bewaakt – samen met de FG – het strategisch beleid en vertaalt externe ontwikkelingen, zoals de Baseline Informatiebeveiliging Overheid (BIO2), de Cbw (implementatie van NIS2) en het IBD Dreigingsbeeld, naar concrete beleidsplannen en jaarplannen. De CISO adviseert gevraagd en ongevraagd het bestuur, de directie en het management over strategische keuzes, risico's en noodzakelijke maatregelen. Adviezen van de CISO zijn zwaarwegend; afwijking hiervan vereist expliciete motivatie en bestuurlijke acceptatie van de (mogelijke) consequenties (risico-acceptatie).

- **Coördinatie en regie**
  De CISO coördineert – samen met de FG – de uitvoering van het strategisch beleid binnen de gemeente, inclusief de afstemming met de Privacy Security Officer, informatieadviseurs en andere relevante collega's. De CISO onderhoudt een overlegstructuur met bestuur, directie en management en draagt bij aan samenhang tussen de verschillende informatiebeveiliging- en privacyrollen. Binnen gemeente Waadhoeke is de CISO tevens verantwoordelijk voor de ENSIA-coördinatie, waardoor de externe verantwoording en het interne beleid optimaal op elkaar aansluiten.

- **Rapportage en verantwoording**
  De CISO rapporteert periodiek over de status van informatiebeveiliging, ontwikkelingen en incidenten aan de burgemeester en het bestuur. Dit gebeurt op basis van actuele ontwikkelingen, incidenten en minimaal via de jaarlijkse ENSIA-audit en een jaarrapportage. Door deze rapportages krijgt het bestuur inzicht in de mate van weerbaarheid en de voortgang van verbetermaatregelen.

- **Risicomanagement en weerbaarheid**
  De CISO monitort en evalueert continu de belangrijkste risico's, met als uitgangspunt het daadwerkelijk verhogen van de digitale weerbaarheid van de gemeente. Het beleid is gericht op het voldoen aan wet- en regelgeving, waaronder de Cbw, maar nadrukkelijk niet op het 'zetten van vinkjes'. Er is ruimte voor innovatie en experimenten, mits deze veilig en verantwoord zijn ingericht. De CISO vertaalt het IBD Dreigingsbeeld en andere relevante analyses naar concrete acties voor de organisatie.

- **Netwerkfunctie en samenwerking**
  De CISO neemt actief deel aan regionale en landelijke netwerken, zoals het CISO-overleg van het Shared Service Centrum Leeuwarden, de Fryske Cybertafel en het CISO-Netwerk Noord-Nederland. Deze samenwerkingen versterken de kennispositie van de gemeente en maken het mogelijk om gezamenlijk te anticiperen op nieuwe dreigingen en ontwikkelingen.

- **Aansturing en samenwerking**
  De CISO werkt in een team met de FG en de PSO. De CISO is het eerste aanspreekpunt voor bestuur en directie bij onderwerpen die gerelateerd zijn aan informatiebeveiliging en stemt af met de informatieadviseurs en andere sleutelfunctionarissen. De aansturing van de Staf vindt plaats door de directeur, maar de CISO heeft korte lijnen naar beide directieleden, de burgemeester, het college en de managers. Dit zorgt voor directe betrokkenheid bij strategische besluitvorming en operationele afstemming.

4.1.2 De Functionaris Gegevensbescherming

De FG is binnen gemeente Waadhoeke de strategisch adviseur en onafhankelijke toezichthouder op het gebied van privacy en gegevensbescherming. De FG ziet toe op de naleving van privacywet- en regelgeving bij de verwerking van persoonsgegevens door of namens de gemeenteraad, het college van burgemeester en wethouders en de burgemeester. De positie en taken van de FG zijn wettelijk verankerd in de artikelen 37, 38 en 39 van de AVG.

Onafhankelijke positionering

De FG opereert volledig onafhankelijk binnen de organisatie. Bestuur, directie, management en medewerkers oefenen geen invloed uit op de uitvoering van zijn taken. De FG heeft – zonder tussenkomst van anderen – toegang tot de hoogste bestuurders (de gemeenteraad, het college van burgemeester en wethouders of de burgemeester) om te adviseren. Bij vraagstukken over gegevensverwerking wordt de FG tijdig en volledig betrokken en krijgt hij toegang tot alle relevante informatie, systemen en processen. Directie en proceseigenaren ondersteunen de FG actief bij het uitvoeren van zijn toezichttaken. Belangenverstrengeling wordt voorkomen door de FG niet te betrekken bij activiteiten of processen waarbij hij verantwoordelijk zou zijn voor gegevensverwerkingen namens de verwerkingsverantwoordelijke. In zijn toezicht houdt de FG rekening met de aard, omvang, context en doeleinden van de verwerkingen en de risico's voor de rechten en vrijheden van betrokkenen.

Kerntaken en verantwoordelijkheden

- **Toezicht op naleving van privacywet- en regelgeving**
  De FG houdt toezicht op de naleving van de AVG en andere relevante privacywetgeving binnen de organisatie. Hij ziet erop toe dat verplichtingen uit de wet- en regelgeving worden nageleefd, verantwoordelijkheden duidelijk zijn toegewezen en risicobeheersmaatregelen daadwerkelijk worden toegepast. De FG monitort of verplichte DPIA's worden uitgevoerd, verzoeken van betrokkenen zorgvuldig worden afgehandeld en of gegevensverwerkingen in samenwerkingsverbanden correct verlopen. Daarnaast bewaakt de FG de behandeling van klachten en signalen over de verwerking van persoonsgegevens vanuit de samenleving en fungeert hij als vast aanspreekpunt voor de AP, inwoners en andere betrokkenen. Zijn bevindingen rapporteert hij aan de verantwoordelijke bestuursorganen.

- **Bewustwording, voorlichting en cultuur**
  Een belangrijk onderdeel van de rol van de FG is het bevorderen van bewustwording en het geven van voorlichting aan medewerkers over privacy en gegevensbescherming. De FG stimuleert een privacybewuste cultuur binnen de organisatie, adviseert over DPIA's en ondersteunt bij het ontwikkelen en implementeren van interne privacy procedures.

- **Informeren en adviseren**
  De FG informeert en adviseert bestuur, directie en/of management periodiek over de stand van zaken rondom gegevensbescherming, actuele ontwikkelingen en incidenten. Dit gebeurt zowel gevraagd als ongevraagd, op zowel strategisch als tactisch niveau. De FG adviseert over beleidsvorming, prioritering en implementatie van privacy maatregelen, DPIA's, geautomatiseerde besluitvorming, internationale doorgifte van gegevens en de omgang met klachten van betrokkenen. Adviezen van de FG zijn zwaarwegend; afwijking hiervan vereist expliciete motivatie en bestuurlijke acceptatie van de (mogelijke) consequenties (risico-acceptatie).

- **Strategie, visie en integrale borging**
  De FG ontwikkelt visie en strategie op het gebied van privacy en gegevensbescherming. De FG ontwikkelt samen met de CISO het strategisch beleid. Hij zoekt naar oplossingsrichtingen, stimuleert normering en zorgt voor integrale borging van privacy in processen en systemen. Door verschillende toezichtsvormen met elkaar te verbinden, levert de FG specialistisch en onafhankelijk advies over complexe privacyvraagstukken en evalueert hij de effectiviteit van het privacybeleid.

- **Netwerkfunctie en samenwerking**
  De FG neemt actief deel aan regionale en landelijke netwerken, zoals het Friese FG-overleg, het FG-overleg van het Shared Service Centrum Leeuwarden, overlegstructuren met samenwerkingspartners zoals DataFryslân, De Dienst Sociale Zaken en Werkgelegenheid Noardwest-Fryslân en de VNG, IBD, Nederlands Genootschap van Functionarissen Gegevensbescherming (NGFG) en de AP. Deze samenwerkingen versterken de kennispositie van de gemeente en maken het mogelijk om gezamenlijk te anticiperen op nieuwe dreigingen en ontwikkelingen.

- **Aansturing en samenwerking**
  De FG werkt in een team met de CISO en de PSO. De FG is het eerste aanspreekpunt voor bestuur, directie en management bij onderwerpen die gerelateerd zijn aan privacy en gegevensbescherming en stemt af met andere sleutelfunctionarissen. De aansturing van de Staf vindt plaats door de directeur, maar de FG heeft korte lijnen naar beide directieleden, de burgemeester, het college en de managers. Dit zorgt voor directe betrokkenheid bij strategische besluitvorming en afstemming.

4.1.3 Privacy Security Officer

De Privacy Security Officer (PSO) is binnen gemeente Waadhoeke verantwoordelijk voor het waarborgen van zowel de bescherming van persoonsgegevens als de informatiebeveiliging. De PSO vervult deze functie organisatiebreed en werkt nauw samen met zowel de FG als de CISO. De PSO ontvangt richting-

gevend advies en instructies van de FG en de CISO en rapporteert periodiek aan beide functionarissen over de voortgang en status van de werkzaamheden.

Positionering en samenwerking
De PSO is het eerste aanspreekpunt voor vraagstukken op het gebied van informatiebeveiliging en privacy. In deze rol fungeert de PSO als verbindende schakel tussen beleid en uitvoering. Door deze positionering is de PSO in staat om zowel het management als medewerkers praktisch te ondersteunen en te adviseren.

Kerntaken en verantwoordelijkheden

- **Rapportage en verantwoording**
  De PSO rapporteert periodiek over de voortgang van beleidsimplementatie op het gebied van informatiebeveiliging en privacy. Dit omvat het rapporteren over incidenten en datalekken, inclusief de opvolging daarvan, en het bieden van inzicht in de status van bewustwording en training binnen de organisatie. Ook de uitvoering binnen de planning- en control cyclus op het gebied van informatiebeveiliging en privacy wordt door de PSO gemonitord en gerapporteerd aan de FG en/of CISO.

- **Beleid en planvorming**
  De PSO stelt uitvoeringsplannen op voor informatiebeveiliging en privacy, beheert en evalueert het bijbehorende beleid, implementatieplannen, procedures en maatregelen, en zorgt voor aansluiting bij het strategisch beleid van de gemeente. Bijzondere aandacht gaat uit naar bewustwording, interne communicatie en de onboarding van (nieuwe) medewerkers, zodat het beleid ook daadwerkelijk wordt nageleefd en verankerd in de organisatie. Daarbij ondersteunt de PSO de implementatie van maatregelen conform de BIO2 en internationale normen zoals ISO 27001/27002.

- **Eerstelijns advisering**
  Als eerste aanspreekpunt voor informatiebeveiliging- en privacyvraagstukken adviseert de PSO bij het opstellen van verwerkersovereenkomsten, convenanten en reglementen. De PSO ondersteunt het management en medewerkers bij de implementatie van maatregelen naar aanleiding van risicoanalyses, DPIA's en incidenten. Verder beantwoordt de PSO vragen of signalen over informatiebeveiliging en gegevensbescherming. Tevens speelt de PSO een actieve rol in het toepassen en onderhouden van de risicomanagementmethodiek binnen de organisatie.

- **Uitvoering en beheer**
  In de uitvoerende rol beheert de PSO diverse systemen en registers, waaronder het verwerkingsregister, datalek- en incidentenregister, risicoregisters en het Information Security Management System (ISMS). De PSO stelt procedures op, voert analyses uit op meldingen en incidenten, monitort audits en assessments en ziet toe op de naleving van beleid en maatregelen. Daarbij ondersteunt de PSO ook het voorbereiden en opvolgen van interne en externe audits.

- **Ondersteuning en samenwerking**
  De PSO biedt ondersteuning bij het uitvoeren van risicoanalyses en DPIA's, de afhandeling van incidenten en de implementatie van privacy- en beveiligingsmaatregelen. Daarnaast is de PSO betrokken bij het toetsen van beveiligingseisen in inkoop- en contractprocessen, conform de BIO2-vereisten. De PSO ondersteunt bij een crisis om de impact van incidenten te beperken en zorgt voor tijdige melding aan toezichthouders. Verder wisselt de PSO kennis en ervaring uit met collega's binnen en buiten de organisatie en onderhoudt contacten met relevante netwerken zoals de IBD, de AP en vakgenoten bij andere gemeenten en overheidsorganisaties.

- **Continu verbeteren**
  De PSO draagt actief bij aan het continu verbeteren van informatiebeveiliging en privacy binnen de gemeente door het toepassen van de PDCA-cyclus. Deze systematische aanpak zorgt voor een voortdurende evaluatie en verbetering van beleid, processen en maatregelen.

4.2 Taken en verantwoordelijkheden per organisatieonderdeel
Informatiebeveiliging en privacy zijn geen geïsoleerde vakgebieden, maar zijn integraal verweven met al onze gemeentelijke taken. Daarom draagt elk organisatieonderdeel binnen gemeente Waadhoeke bij aan het beschermen van informatie en persoonsgegevens, elk vanuit de eigen rol en verantwoordelijkheden. Van college tot medewerker loopt er een doorlopende lijn van verantwoordelijkheid. Het college zet de strategische koers uit en toont voorbeeldgedrag, de directie vertaalt dit naar tactische sturing en risicomanagement, afdelingsmanagers nemen eigenaarschap binnen hun processen en medewerkers maken het dagelijks waar door procedures te volgen en incidenten te melden. Dit zorgt ervoor dat informatiebeveiliging en privacy geen remmende verplichtingen worden, maar een integraal onderdeel zijn van goed bestuur en betrouwbare dienstverlening.

4.2.1 College van burgemeester en wethouders

- **Strategische koers**
  Het college draagt de eindverantwoordelijkheid voor het strategisch beleid van gemeente Waadhoeke. Zij stelt het beleidskader vast, hanteert de tien principes voor informatiebeveiliging en de beginselen voor verwerking van persoonsgegevens en borgt dat informatiebeveiliging en privacy blijvend aandacht krijgen in de bestuurlijke agenda. Het college stelt de benodigde middelen beschikbaar en borgt dat capaciteit, budget en prioriteit voor informatiebeveiliging en privacy jaarlijks onderdeel zijn van de begrotingscyclus.

- **Leiderschap en voorbeeldgedrag**
  Burgemeester en wethouders tonen zichtbaar voorbeeldgedrag door zelf conform de vastgestelde regels te handelen. Zij vragen actief om rapportages over de actuele stand van zaken, zodat zij tijdig kunnen bijsturen en prioriteren. Daarmee creëren zij een cultuur waarin veiligheid en privacy vanzelfsprekend zijn.

4.2.2 Directie

- **Positionering en regie**
  De directie vertaalt het strategisch beleid naar concrete sturing en toezicht. Iedere gegevensverzameling, elk proces en systeem valt onder de verantwoordelijkheid van een afdelingsmanager; de directie wijst deze eigenaar formeel toe en houdt toezicht op naleving.

- **Agendering**
  De directie benadrukt bij aanstelling en interne overplaatsing en bijvoorbeeld in werkoverleggen of in personeelsgesprekken met de managers het belang van opleiding en training voor informatiebeveiliging en privacy. De directie stimuleert hen actief deze periodiek te volgen.

- **Beleidsvorming en autorisatie**
  De directie stelt aanvullende onderwerp specifieke beleidsdocumenten op tactisch en operationeel niveau vast. Daarnaast autoriseert ze procedures en maatregelen die nodig zijn voor de bescherming van informatie en persoonsgegevens. En werkt hierin nauw samen met de CISO en FG.

- **Toezicht en verantwoording**
  De directie verzamelt periodiek informatie bij het management over de voortgang en effectiviteit van genomen maatregelen. Zij rapporteert – gevraagd en ongevraagd – aan de portefeuillehouders in het college en zorgt dat het bestuur zich adequaat kan verantwoorden richting gemeenteraad.

- **Risicomanagement**
  Informatiebeveiliging en privacy zijn een vast onderdeel van de reguliere risicomanagementcyclus. De directie bewaakt het gewenste niveau van continuïteit en vertrouwelijkheid en ziet erop toe dat significante risico's worden gemitigeerd of expliciet geaccepteerd. De directie bepaalt, op voorstel van CISO en FG, het resterende restrisico dat de organisatie kan accepteren en documenteert dit besluit.

4.2.3 Management (programma- en afdelingsmanagers)

- **Eigenaarschap van processen en gegevens**
  Managers zijn eindverantwoordelijk voor bescherming van informatie en persoonsgegevens binnen hun domein. Deze verantwoordelijkheid is niet overdraagbaar. Uitvoering van specifieke taken kan wel worden gedelegeerd. Bijvoorbeeld aan teamleiders of medewerkers. Voor elke applicatie, dataset of basisregistratie is er altijd een aantoonbare interne eigenaar. Voor elk proces is een proceseigenaar benoemd die ook verantwoordelijk is voor het actualiseren van de procesbeschrijving bij iedere proces- of systeemwijziging.

- **Inbedding in dagelijkse praktijk**
  Managers zorgen dat informatiebeveiliging en privacy structureel zijn geïntegreerd in processen, systemen en dienstverlening. Zij houden het verwerkingsregister actueel, oefenen scenario's rond incidenten en bedrijfscontinuïteit en voeren periodiek controles uit zodat uitsluitend bevoegde medewerkers toegang hebben tot de juiste gegevens. Zij reserveren binnen hun afdelingsbudget structureel middelen voor het implementeren van maatregelen.

- **Agendering**

Minimaal twee keer per jaar staan informatiebeveiliging en privacy op de agenda van het Management Overleg (MO). Daarnaast komt het onderwerp expliciet aan bod in (programma- en afdelings)plannen wanneer risico's daar aanleiding toe geven.

- **Risico-gestuurde maatregelen**
  Op basis van risicoanalyses, (pre-)DPIA's, incidentanalyses, overige signalen of advies van het IB&P-team bepalen managers passende maatregelen. Afwijkingen van verplichte controls of beginselen worden altijd afgestemd met de CISO en/of FG. Zij documenteren de beslissingen en restrisico's in het risicoregister zodat deze zichtbaar zijn voor de directie, CISO en FG.

- **Cultuur, bewustwording en training**
  Het management benadrukt bij aanstelling en interne overplaatsing en bijvoorbeeld in werkoverleggen of in personeelsgesprekken met de medewerkers het belang van opleiding en training voor informatiebeveiliging en privacy. Het management stimuleert hen actief deze periodiek te volgen.

- **Samenwerking en signalering**
  Managers dragen het beleid actief uit, signaleren nieuwe dreigingen en betrekken CISO, FG en Privacy Security Officer vroegtijdig bij proces- of systeemwijzigingen.

- **Wet- en regelgeving**
  Managers waarborgen naleving van (U)AVG, BIO2, Cbw en overige relevante kaders binnen alle processen en systemen.

4.2.4 Medewerkers

- **Persoonlijke verantwoordelijkheden**
  Elke medewerker behandelt informatie en persoonsgegevens zorgvuldig, volgt vastgestelde procedures en houdt zich aan de gestelde kaders. Medewerkers gebruiken uitsluitend geautoriseerde systemen, kiezen sterke wachtwoorden en delen gegevens alleen als dit noodzakelijk en toegestaan is en op een veilige manier kan. Zij vergrendelen hun beeldscherm wanneer zij hun werkplek verlaten en nemen bij twijfel altijd contact op met het IB&P-team.

- **Informatiebeveiligingsincident of datalek**
  Bij een vermoeden van informatiebeveiligingsincident, een datalek, verlies van gegevens of misbruik melden zij dit direct via het interne meldproces, zodat de organisatie snel kan ingrijpen en rapporteren. Medewerkers volgen daarbij de interne procedure 'Melding beveiligingsincident en datalekken' en gebruiken het daarvoor bedoelde meldportaal.

- **Kennis en vaardigheid**
  Medewerkers nemen deel aan verplichte bewustwordingsprogramma's, actualiseren hun kennis wanneer wet- of regelgeving verandert en passen geleerde maatregelen consequent toe.

- **Samenwerking**
  Zij werken actief samen met collega's, CISO, FG en PSO om risico's te signaleren, te voorkomen, te mitigeren en best practices te delen.

Bijlage 1. RASCI-tabel Informatiebeveiliging

Baseline Informatiebeveiliging Overheid (BIO) 2		Rollen en verantwoordelijkheden					
Onderwerp	**Control**	**College**	**Directie**	**Manager**	**CISO**	**FG**	**PSO**
Organisatorische Beheersmaatregelen							
Beleidsregels voor informatiebeveiliging	5.01	A	R	R	S	C	C/S
Rollen en verantwoordelijkheden bij informatiebeveiliging	5.02	A	R	R	S	C	C/S
Functiescheiding	5.03	I	A	R			
Bewustwording, opleiding en training in informatiebeveiliging	5.04	I	A	R	C	C	C
Contact met overheidsinstanties	5.05	I	A	R	S	S	C/S
Contact met speciale belangengroepen	5.06	I	A	R	R	R	R
Informatie en analyses over dreigingen	5.07	I	A	R	C	C	C
Informatiebeveiliging in projectmanagement	5.08	I	A	R	C	I	C
Inventarisatie van informatie en andere gerelateerde bedrijfsmiddelen	5.09	I	A	R	C	C	C
Aanvaard gebruik van informatie en andere gerelateerde bedrijfsmiddelen	5.10	I	A	R	C	C	C
Retourneren van bedrijfsmiddelen	5.11	I	A	R	C		C
Classificeren van informatie	5.12	I	A	R	C	C	C
Labelen van informatie	5.13	I	A	R	C	C	S
Overdragen van informatie	5.14	I	A	R	C	C	S
Toegangsbeveiliging	5.15	I	A	R	C	C	S
Identiteitsbeheer	5.16	I	A	R	C	I	S
Authenticatie-informatie	5.17	I	A	R	C	I	S
Toegangsrechten	5.18	I	A	R	C	C	S
Informatiebeveiliging in leveranciersrelaties	5.19	I	A	R	C	C	C/S
Adresseren van informatiebeveiliging in leveranciersovereenkomsten	5.20	I	A	R	C	I	C/S
Beheren van informatiebeveiliging in de ICT-toeleveringsketen	5.21	I	A	R	C	I	C/S
Monitoren, beoordelen en het beheren van wijzigingen van leveranciersdiensten	5.22	I	A	R	C	I	S
Informatiebeveiliging voor het gebruik van clouddiensten	5.23	I	A	R	C	C	S
Plannen en voorbereiden van het beheer van informatiebeveiligingsincidenten	5.24	I	A	R	C	C	S
Beoordelen van en besluiten over informatiebeveiligingsgebeurtenissen	5.25	I	A	R	C	C	C/S
Reageren op informatiebeveiligingsincidenten	5.26	I	A	R	C	C	S
Leren van informatiebeveiligingsincidenten	5.27	I	A	R	C	C	C/S
Verzamelen van bewijsmateriaal	5.28	I	A	R	C	C	S
Informatiebeveiliging tijdens een verstoring	5.29	I	A	R	C	I	C
ICT-gereedheid voor bedrijfscontinuïteit	5.30	I	A	R	C	I	C
Wettelijke, statutaire, regelgevende en contractuele eisen	5.31	I	A	R	C	I	S
Intellectuele-eigendomsrechten	5.32	I	A	R	C		S

Bewaartermijnen en naleving	5.33	I	A	R	C	I	S
Privacy en bescherming van persoonsgegevens	5.34	I	A	R	C	S	C/S
Onafhankelijke beoordeling van informatiebeveiliging	5.35	I	A	R	C	I	S
Naleving van beleid, regels en normen voor informatiebeveiliging	5.36	I	A	R	S	I	C
Gedocumenteerde bedieningsprocedures	5.37	I	A	R	C		
Mensgerichte beheersmaatregelen							
Screening	6.01	I	A	R	C	C	C
Arbeidsovereenkomst	6.02	I	A	R	C	I	C
Bewustwording van, opleiding en training in informatiebeveiliging	6.03	I	A	R	C	C	C
Disciplinaire procedure	6.04	I	A	R	C	I	C
Verantwoordelijkheden na beëindiging of wijziging van het dienstverband	6.05	I	A	R	C	I	S
Vertrouwelijkheids- of geheimhoudingsovereenkomsten	6.06	I	A	R	C	C	C
Werken op afstand	6.07	I	A	R	S	I	S
Melden van informatiebeveiligingsgebeurtenissen	6.08	I	A	R	C	C	C/S
Fysieke beheersmaatregelen							
Fysieke beveiligingszones	7.01	I	A	R	C	I	S
Fysieke toegangsbeveiliging	7.02	I	A	R	C	I	S
Beveiligen van kantoren, ruimten en faciliteiten	7.03	I	A	R	C	I	S
Monitoren van de fysieke beveiliging	7.04	I	A	R	C	I	S
Beschermen tegen fysieke en omgevingsdreigingen	7.05	I	A	R	C	I	S
Werken in beveiligde zones	7.06	I	A	R	C	I	S
'Clear desk' en 'clear screen'	7.07	I	A	R	C	I	S
Plaatsen en beschermen van apparatuur	7.08	I	A	R	C	I	S
Beveiligen van bedrijfsmiddelen buiten het terrein	7.09	I	A	R	C		S
Opslagmedia	7.10	I	A	R	C	I	S
Nutsvoorzieningen	7.11	I	A	R	C		S
Beveiligen van bekabeling	7.12	I	A	R	C		S
Onderhoud van apparatuur	7.13	I	A	R	C		S
Veilig verwijderen of hergebruiken van apparatuur	7.14	I	A	R	C		S
Technologische beheersmaatregelen							
User endpoint devices	8.01	I	A	R	S		S
Speciale toegangsrechten	8.02	I	A	R	C	I	S
Beperking toegang tot informatie	8.03	I	A	R	C	I	C/S
Toegangsbeveiliging op broncode	8.04	I	A	R	C		S
Beveiligde authenticatie	8.05	I	A	R	C	I	S
Capaciteitsbeheer	8.06	I	A	R	C		S
Bescherming tegen malware	8.07	I	A	R	C	I	S
Beheer van technische kwetsbaarheden	8.08	I	A	R	C	I	S
Configuratiebeheer	8.09	I	A	R	C		S
Wissen van informatie	8.10	I	A	R	C	I	S
Maskeren van gegevens	8.11	I	A	R	C	I	S

Voorkomen van gegevenslekken (data leakage prevention)	8.12	I	A	R	C	I	S
Back-up van informatie	8.13	I	A	R	C	I	S
Redundantie van informatieverwerkende faciliteiten	8.14	I	A	R	C	I	S
Logging	8.15	I	A	R	C	C	S
Monitoren van activiteiten	8.16	I	A	R	C	I	S
Kloksynchronisatie	8.17	I	A	R	C		S
Gebruik van speciale systeemhulpmiddelen	8.18	I	A	R	C		S
Installeren van software op operationele systemen	8.19	I	A	R	C	I	S
Beveiliging netwerkcomponenten	8.20	I	A	R	C	I	S
Beveiliging van netwerkdiensten	8.21	I	A	R	C	I	S
Netwerksegmentatie	8.22	I	A	R	C	I	S
Toepassen van webfilters	8.23	I	A	R	C	I	S
Gebruik van cryptografie	8.24	I	A	R	C	C	S
Beveiligen tijdens de ontwikkelcyclus	8.25	I	A	R	C		S
Toepassingsbeveiligingseisen	8.26	I	A	R	C	I	S
Veilige systeemarchitectuur en technische uitgangspunten	8.27	I	A	R	C	I	S
Veilig coderen	8.28	I	A	R	C		S
Testen van de beveiliging tijdens ontwikkeling en acceptatie	8.29	I	A	R	C	I	S
Uitbestede systeemontwikkeling	8.30	I	A	R	C	I	S
Scheiden van ontwikkel-, test- en productieomgevingen	8.31	I	A	R	C	I	S
Wijzigingsbeheer	8.32	I	A	R	C		S
Testgegevens	8.33	I	A	R	C	C	S
Bescherming van informatiesystemen tijdens audits	8.34	I	A	R	C	I	S
OT-beheersmaatregelen							
Inventarisatie en classificatie van alle OT-assets	OT.01	I	A	R	S		C/S
Segmentatie tussen IT- en OT-netwerken is geïmplementeerd en geborgd	OT.02	I	A	R	S		C/S
Toegangsbeheer en logging op OT-systemen zijn ingericht	OT.03	I	A	R	S		C/S
OT-systemen worden gepatcht en beveiligd onderhouden	OT.04	I	A	R	S		C/S
Leveranciers en remote access tot OT zijn gecontroleerd en vastgelegd	OT.05	I	A	R	S		C/S
Kwetsbaarheden in OT-systemen worden bewaakt en verholpen	OT.06	I	A	R	S		C/S
Monitoring en detectie op afwijkend OT-verkeer is ingericht	OT.07	I	A	R	S		C/S
Back-up en herstelprocedures voor OT zijn getest	OT.08	I	A	R	S		C/S
OT-incidenten volgen het reguliere incidentproces	OT.09	I	A	R	S		C/S
OT-risicoanalyse wordt jaarlijks uitgevoerd en geëvalueerd	OT.10	I	A	R	S		C/S

Bijlage 2. RASCI-tabel Privacy

Algemene Verordening Gegevensbescherming (AVG Borgingsproduct 3.0)		Rollen en verantwoordelijkheden					
Onderwerp	**Control**	**Colle-ge**	**Direc-tie**	**Mana-ger**	**CISO**	**FG**	**PSO**
Beleid	1						
Er is beleid om beleid vast te stellen	1.1	A	R	R	C	C	C
Er is een algemeen privacybeleid en uitwerkingen daarvan	1.2	A	R	R	C	C	C
Verantwoordelijkheden op het niveau van het lijnmanagement zijn benoemd, belegd en vastgelegd. (TVB Matrix/RAS-CI Tabel)	1.3	A	R	R	C	C	C
Risico's	1.4	A	R	R	C	C	C
Processen	2						
Operationele processen	2.1		A	R	C	C	C
Verwerkingsregister	2.3		A	R	C	C	C
Naleving	2.2	I	A	R	C	C	C
DPIA's	2.4	I	A	R	C	C	C
Schonen	2.5		A	R	C	C	C
Organieke Inbedding	3						
Aanstelling en positie FG	3.1	I	A	R	C		C
Privacyteam	3.2	I	A	R	C	C	C
Informeren OR	3.3		A	R	C	C	C
Bewustwording	3.4	I	A	R	C	C	C
Rechten van betrokkenen	4						
Processen rechten van betrokkene op orde	4.1		A	R		C	C
Informatieplicht	4.2	I	A	R	C	C	C
Toestemming	4.3		A	R		C	C
Geautomatiseerde individuele besluit-vorming	4.4		A	R		C	C
Transparantie	4.5		A	R		C	C
Privacy- en cookieverklaring	4.6		A	R	C	C	C
Technische ondersteuning	4.7		A	R		C	C
Samenwerking	5						
De organisatie heeft inzichtelijk welke AVG-rol externe partijen innemen en er worden afspraken gemaakt conform de AVG.	5.1		A	R	C	C	C
Eenmalige gegevensverstrekkingen worden getoetst aan de relevante privacywet- en regelgeving.	5.2		A	R	C	C	C
Beveiliging	6						
Gegevens bescherming door ontwerp	6.1		A	R	C	C	C
Gegevensbescherming door standaard instellingen	6.2		A	R	C	C	C
Datalekken	6.3	I	A	R	C	C	C
Informatiebeveiliging	6.4	A	R	R	C	C	C
Verantwoording	7						
Evaluatie naleving AVG	7.1	I	A	R	C	C	C
Rapportage	7.2	I	A	R	C	C/R	C/R