GEMEENTE LOPIK

# GEMEENTEBLAD

Officiële uitgave van de gemeente Lopik

Nr. 46049

30 januari 2024

## Strategisch informatiebeveiligings- en privacybeleid gemeente Lopik 2023-2026

Het college van burgemeester en wethouders van de gemeente Lopik,

gezien het advies van de afdeling Bedrijfsvoering van 13 december 2023;

**besluit:**

Het Strategisch InformatieBeveiligings- en Privacybeleid en het Tactisch Privacybeleid voor de periode 2023 – 2026 vaststellen.

### 1. Inleiding

Deze beleidsnota beschrijft het strategisch InformatieBeveiligings- en Privacybeleid (IBP-beleid) voor de jaren 2023-2026 van de gemeente Lopik. Het vervangt het in 2018 vastgestelde 'Gemeentelijk Informatiebeveiligingsbeleid 2018-2021'. Deze nota is richtinggevend en kaderstellend en wordt aangevuld met specifieke beleidsdocumenten op tactisch niveau (domeinspecifiek beleid, procedures) en werkinstructies op operationeel niveau. De uitwerking van het beleid in concrete maatregelen en activiteiten wordt vastgelegd in het InformatieBeveiligings- en Privacyplan (IBP-plan). Dit plan wordt jaarlijks bijgewerkt.

Dit IBP-beleid is een verantwoordelijkheid van het bestuur van de Gemeente Lopik. De bestuurders en het MT van de Gemeente Lopik zullen volgens de 10 principes voor informatiebeveiliging (zie paragraaf 2.2.4) richting en sturing geven aan het onderwerp informatiebeveiliging en privacybescherming door het geven van voorbeeldgedrag en het vragen om informatie.

#### 1.1 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 (juistheid) en vertrouwelijkheid ten aanzien van bedrijfsinformatie en persoonsgegevens.

#### 1.2 Privacy & Gegevensbescherming (AVG en Wet politiegegevens)

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

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

#### 1.3 Ambitie en visie van de gemeente Lopik op het gebied van informatieveiligheid en privacybescherming

De gemeente Lopik heeft als ambitie om kwalitatief goede dienstverlening te leveren.
Informatie is bij deze dienstverlening een belangrijk hulpmiddel. De waarborging van de kwaliteit van deze informatie is ons uitgangspunt. Het voldoen aan de wetten en normen voor informatieveiligheid en privacybescherming is hierbij randvoorwaardelijk.

Persoonlijke en gevoelige gegevens van inwoners en ondernemers worden toevertrouwd aan de lokale overheid. Zij moeten erop kunnen vertrouwen dat die informatie bij de lokale overheid in veilige handen is. Ons doel is om de bescherming van de privacy van onze inwoners in te richten volgens de meest passende normen van informatiebeveiliging. Wij volgen daarom trends en ontwikkelingen op de voet. Daarom blijven wij investeren in kennis en kunde. Zo kunnen wij actuele vraagstukken rondom privacy en informatieveiligheid zo goed mogelijk aanpakken.

Onze ambitie is dat:
1. De gemeente Lopik digitaal veilig is: medewerkers zijn zich bewust van de risico's voor informatieveiligheid en de technische voorzieningen zijn op orde ter voorkoming van cybercriminaliteit, zodat schade door verstoring of uitval van ICT geminimaliseerd wordt.
2. De gemeente Lopik is digitaal weerbaar doordat het potentiële dreigingen en incidenten vroegtijdig kan signaleren en de gevolgen ervan kan voorkomen dan wel beperken.
3. De gemeente Lopik beschermt de persoonsgegevens: medewerkers gaan bewust om met persoonsgegevens door deze alleen te gebruiken wanneer dit noodzakelijk is en door de persoonsgegevens om een juiste en veilige wijze op te slaan, te beheren, te archiveren en te vernietigen

Als gemeente Lopik willen we, op basis van risicomanagement, de regierol vervullen om samen met de regionale ketenpartners (WIL, RBL, RUD, BGHU) en ICT-leveranciers de geconstateerde risico's door informatiebeveiligingsmaatregelen te verminderen.

Met dit IBP-beleid zet de gemeente een volgende stap om de beveiliging van persoonsgegevens en andere informatie binnen de gemeente te continueren en voort te gaan op de stappen die in de voorgaande jaren gezet zijn.

### 1.4 Leeswijzer
In hoofdstuk 2 wordt de kern van het IBP-beleid uiteengezet. Hoofdstuk 3 beschrijft vervolgens hoe de taken en verantwoordelijkheden in de organisatie belegd zijn.

## 2. Strategisch beleid
### 2.1 Doelstelling
De strategische doelen van het IBP-beleid zijn:
- Het managen van de informatiebeveiliging.
- Adequate bescherming van bedrijfsmiddelen en persoonsgegevens.
- Het toepassen van dataminimalisatie.
- Het minimaliseren van risico's van menselijk gedrag.
- Het voorkomen van ongeautoriseerde toegang.
- Het garanderen van correcte en veilige informatievoorzieningen.
- Het beheersen van de toegang tot informatiesystemen.
- Het waarborgen van veilige informatiesystemen.
- Het adequaat reageren op incidenten.
- Het beschermen van (kritieke) bedrijfsprocessen.
- Het beschermen en correct verwerken van persoonsgegevens van burgers en medewerkers.
- Voldoen aan de wettelijke verplichtingen voortvloeiend uit de AVG en dit op ieder moment met bewijs kunnen aantonen
- Het waarborgen van de naleving van dit beleid.

### 2.2 Aanleidingen voor het aanpassen van het beleid
Dit beleidsdocument wordt periodiek beoordeeld. Bij grote en relevante wijzigingen met betrekking tot informatieveiligheid wordt het beleid geactualiseerd. Minimaal wordt het van kracht zijnde beleid elke 4 jaar geactualiseerd en, na een juridische toets, aangeboden ter goedkeuring.
Het college van B en W stelt als eindverantwoordelijke voor de informatiebeveiliging het strategisch IBP-beleid vast. Wijzigingen in het beleid worden via de gebruikelijke kanalen gecommuniceerd binnen en buiten de organisatie. Eerdere versies worden in het documentmanagementsysteem verwijderd in overeenstemming met het vastgestelde bewaarschema.
Het actualiseren van dit document volgt de meerjarige planning & control-cyclus om daarmee de aansluiting te borgen van informatieveiligheidsdoelstellingen op beleidswijzigingen en strategische doelstellingen van de Gemeente Lopik.
In de paragrafen hieronder worden de wijzigingen beschreven ten opzichte van het voorgaande beleidsdocument.

#### 2.2.1 De BIO
Voor de ondersteuning van gemeenten bij het formuleren en realiseren van hun informatiebeveiligingsbeleid heeft de interbestuurlijke werkgroep Normatiek[1] in 2018 de Baseline Informatiebeveiliging Overheid (BIO) uitgebracht. De basis hiervoor is de NEN-ISO/IEC 27001:2017. De beveiligingsmaatregelen worden op basis van de NEN-ISO/IEC 27002:2017 en best practices bij (lokale) overheden genomen.

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

De BIO is sinds 2019 het normenkader voor de gehele overheid. Het bestaat uit een baseline met verschillende niveaus van beveiligen. Aanvullend hierop worden praktische operationele handreikingen uitgebracht, zoals een handleiding voor het uitvoeren van een risicoanalyse voor het opstellen van een beveiligingsplan.

In opzet is de BIO een kwaliteitssysteem, waarbij jaarlijks het niveau van beveiliging wordt verbeterd via een PDCA-cyclus (Plan-Do-Check-Act). Op basis van een inschatting door het lijnmanagement van mogelijke dreigingen en schade worden beveiligingsmaatregelen genomen die de risico's beperken. De Cybersecurity Implementatie Richtlijn (CSIR) is een afgeleide van de BIO, speciaal voor de beveiliging van procesautomatisering, bijvoorbeeld voor pompen en gemalen.

### 2.2.2 De AVG

Nieuwe technologische ontwikkelingen, innovatieve voorzieningen, globalisering en een steeds digitaler wordende overheid maakt het zorgvuldig omgaan met persoonsgegevens steeds complexer en noodzakelijker. De gemeente Lopik is zich hiervan bewust en wil daarom met dit beleid aangeven hoe zij in algemene zin invulling geeft aan nationale en Europese wet- en regelgeving op het gebied van privacy, waaronder de Algemene Verordening Gegevensbescherming (AVG). Het AVG Borgingsproduct, ontwikkeld door de InformatieBeveiligingsDienst (IBD, een onderdeel van de VNG), dient hierbij als toetsingskader.

### 2.2.3 De WPG

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

### 2.2.4 De 10 principes voor informatiebeveiliging[2]

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

1. Bestuurders bevorderen een veilige cultuur.
2. Informatiebeveiliging 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 controleert en evalueert.

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

### 2.2.5 Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten

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

### 2.2.6 Informatie uit incidenten, inbreuken op de beveiliging en datalekken

De gemeente Lopik heeft een eigen systeem waarin incidenten en datalekken worden vastgelegd. Deze informatie is waardevol als input bij het actualiseren van het beleid.

### 2.3 Scope strategisch beleid

De scope van dit beleid omvat alle gemeentelijke procedures, 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.

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

Het borgt daarmee de informatievoorziening en de bescherming van persoonsgegevens gedurende de hele levenscyclus van informatiesystemen, ongeacht de toegepaste technologie (ICT of OT: Operationele Technologie voor de procesautomatisering).

Dit IBP-beleid is een algemene basis en dekt tevens aanvullende beveiligingseisen uit wet- en regelgeving af, zoals voor de AVG, UAVG, WPG, BRP, PNIK/PUN, DigiD en SUWI. Deze worden in aanvullende documenten verder uitgewerkt.

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

**2.4 Uitgangspunten strategisch beleid**
Het college van B en W en het lijnmanagement (Management Team) spelen een cruciale rol bij het uitvoeren van dit strategische IBP-beleid. Het management maakt een inschatting van het belang dat de verschillende delen van de informatievoorziening voor de gemeente heeft, de (privacy-)risico's die de gemeente hiermee loopt en welke van deze risico's onacceptabel hoog zijn.
Op basis hiervan zet het management dit beleid voor informatiebeveiliging en privacy op, draagt dit uit naar de organisatie en ondersteunt en bewaakt de uitvoering ervan.

Het gemeentelijk management geeft door het uitdragen en handhaven van het IBP-beleid een duidelijke richting aan en demonstreert dat zij informatiebeveiliging en privacybescherming ondersteunt en zich hierbij betrokken voelt. Het IBP-beleid is in lijn met het algemene beleid van de gemeente en de relevante landelijke en Europese wet- en regelgeving.

De belangrijkste uitgangspunten van het beleid zijn:
- De uitvoering van de informatiebeveiliging en privacybescherming is een verantwoordelijkheid van het lijnmanagement. Alle informatiebronnen en -systemen die gebruikt worden door de gemeente Lopik hebben een interne eigenaar die de vertrouwelijkheid, privacy-eisen en/of waarde bepaalt van de informatie die ze bevatten. De primaire verantwoordelijkheid voor de bescherming van informatie ligt dan ook bij deze interne eigenaar van de informatie.
- Het borgen van de informatiebeveiliging en privacybescherming vindt risicogestuurd plaats. De verantwoordelijken in de organisatie maken afwegingen ter naleving van de normenkaders en op basis van een risico-inschatting.
- Informatiebeveiliging en privacybescherming is een continu verbeterproces. 'Plan, do, check en act' vormen samen het managementsysteem van informatiebeveiliging. Door periodieke controle, organisatiebrede planning én coördinatie wordt de kwaliteit van de informatievoorziening en privacy verankerd binnen de organisatie.
- Het IBP-beleid vormt samen met het IBP-plan het fundament onder een betrouwbare informatievoorziening en privacybescherming. Het IBP-plan wordt periodiek bijgesteld op basis van nieuwe ontwikkelingen, registraties in het incidentenregister en bestaande risicoanalyses.
- Vastgestelde beleidsstukken en uitwerkingen daarvan (bijv. procedures, standaarden en werkinstructies) worden centraal beheerd in het managementsysteem voor informatiebeveiliging en privacybescherming.
- Regels en verantwoordelijkheden voor het (aanvullend) strategische IBP-beleid dienen te worden vastgelegd en vastgesteld en gecommuniceerd aan medewerkers en relevante externe partijen.
- Alle informatie en informatiesystemen zijn van belang voor de gemeente, bepaalde informatie is zelfs van vitaal en kritiek belang. Hoewel de basisregistraties (zoals BRP, WOZ, BAG, BGT, BRO) en kernregistraties belangrijk zijn in het kader van informatiebeveiliging, krijgen zij niet meer of minder voorrang dan andere (primaire) processen binnen de gemeente. Het samenspel van alle processen binnen de bedrijfsvoering is belangrijk voor de missie en de visie van de gemeente en het behalen van de doelen die zijn gesteld.
- Alle Proces Automatiseringssystemen (PA) die binnen de gemeentelijke gebouwen en in de publieke ruimte van de gemeente worden gebruikt, die van de gemeente zijn, zoals gebouwbeheersingssystemen en bijvoorbeeld camera-technologie of pompen en gemalen, dienen beveiligd te worden conform de Cybersecurity Implementatie Richtlijn (CSIR).
- De gemeente stelt de benodigde mensen en middelen beschikbaar om haar eigendommen en werkprocessen te kunnen beveiligen en te voldoen aan de privacy-eisen volgens de wijze zoals gesteld in dit beleid.
- Iedere medewerker, zowel vast als tijdelijk, intern of extern, is verplicht waar nodig (persoons)gegevens en informatiesystemen te beschermen tegen ongeautoriseerde toegang, gebruik, verandering, openbaring, vernietiging, verlies of overdracht en bij vermeende inbreuken hiervan melding te maken. Daarvoor worden medewerkers getraind in het gebruik van beveiligingsprocedures en hebben zij in een bewustwordingsprogramma de benodigde basiskennis opgedaan van informatiebeveiliging en privacywetgeving.

### 2.5 Randvoorwaarden

Belangrijke randvoorwaarden zijn:

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

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

## 3. Organisatie, taken & verantwoordelijkheden

In dit hoofdstuk wordt uiteengezet welke taken en verantwoordelijkheden met betrekking tot informatiebeveiliging en privacybescherming 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 is de eerste lijn verantwoordelijk voor het realiseren van informatiebeveiliging en privacy binnen de eigen processen. De tweede lijn ondersteunt, adviseert, coördineert en bewaakt of de eerste lijn de verantwoordelijkheden ook daadwerkelijk neemt. In de derde lijn wordt het geheel van een objectief oordeel voorzien met mogelijkheden tot verbetering.

### 3.1 De 1e lijn: aansturing en uitvoering

De directie:

- Stuurt aan op het nemen van adequate maatregelen voor de bescherming van de informatie, informatiesystemen en procesautomatiseringsystemen die onder hun verantwoordelijkheid valt.
- Stelt het gewenste niveau van continuïteit en vertrouwelijkheid vast.
- Draagt zorg voor het uitwerken van tactische informatiebeveiligings- en privacybeleidsonderwerpen die aanvullend zijn op het strategisch beleid en laat zich hierin bijstaan door de functionarissen uit de “second line of defense”.
- Stelt jaarlijks het IBP-plan vast en autoriseert de benodigde procedures en uitvoeringsmaatregelen.
- Zorgt dat de teamleiders jaarlijks verantwoording afleggen over de beveiliging van de informatie die onder hen berust.
- Zorgt dat de eindverantwoordelijke portefeuillehouders binnen het college gevraagd en ongevraagd geïnformeerd wordten over de informatiebeveiliging.

De teamleiders:

- Zorgen voor de uitvoering van de informatiebeveiliging en de borging van de AVG binnen de processen waarvoor zij verantwoordelijk zijn.
- Zijn verantwoordelijk voor het oefenen met informatiebeveiligings- en privacy-incidenten en bedrijfscontinuïteit.
- Voeren risicoanalyses informatiebeveiliging uit op basis van de BIO en bij verwerken van persoonsgegevens tevens (Pre-)DPIA’s op basis van de AVG.
- Dragen het IBP-beleid en de daaraan gerelateerde procedures uit.
- Zorgen er voor dat informatiebeveiliging en privacybescherming deel uit maken van de beoordelingssystematiek en worden besproken tussen de leidinggevende en de medewerker.
- Zien erop toe dat de controle op het verwerken van persoonsgegevens regelmatig wordt uitgevoerd, zodat kan worden vastgesteld dat alleen bevoegde ambtenaren de juiste persoonsgegevens ingezien en verwerkt hebben.
- Leveren een actieve bijdrage aan de informatiebeveiliging en privacybescherming door bedreigingen vroegtijdig te signaleren, input te leveren voor wijzigingen op maatregelen en procedures, bespreken van de beveiligingsincidenten en privacy-inbreuken met de functionarissen uit de “second line of defense”.

### 3.2 De 2e lijn: ondersteuning

#### 3.2.1 Chief Information Security Officer (CISO)
De CISO is verantwoordelijk voor het implementeren van en toezicht houden op het informatiebeveiligingsbeleid.
De CISO ondersteunt vanuit een onafhankelijke positie de organisatie bij het bewaken en verhogen van de betrouwbaarheid van de informatievoorziening en rapporteert hierover rechtstreeks aan het MT.

#### 3.2.2 Privacy Officer (PO)
De PO is verantwoordelijk voor het actualiseren en bewaken van het privacybeleid binnen de gemeente. De PO heeft een operationeel uitvoerende rol en is het dagelijkse aanspreekpunt voor medewerkers wat betreft gegevensbescherming. Daar passen taken bij als adviseren over de procedures en de werkprocessen binnen de teams, over het afsluiten van (verwerkers)overeenkomsten met externe partijen, het beheer van het register van verwerkingen en het coördineren van het proces rond datalekken. De PO heeft een adviserende rol bij het in beeld brengen van privacy risico's door middel van DPIA's.

### 3.3 De 3e lijn: controle en verantwoording

#### 3.3.1 ENSIA-coördinator en de Register EDP Auditor (RE)
De gemeente verantwoordt zich over informatiebeveiliging via de ENSIA-systematiek. Daarvoor is een ENSIA-team opgericht. De ENSIA-coördinator wordt jaarlijks aangewezen. Deze coördineert de acties die nodig zijn voor het invullen van de ENSIA-vragenlijsten. De leden van het ENSIA-team rapporteren de resultaten naar de betrokken teamleiders.

De ingevulde zelfevaluatievragenlijst vormt de basis voor het opstellen van de collegeverklaring aan de raad. Deze verklaring wordt na goedkeuring ondertekend door een RE Auditor. 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 en wettelijke eisen zoals uit de AVG. Ook worden de eventuele verbetermaatregelen vermeld die de gemeente gaat treffen.

Via de jaarlijkse collegeverklaring Informatiebeveiliging worden het bestuur van de Gemeente Lopik en de raad geïnformeerd. De betrokkenheid van het bestuur is essentieel. Hiermee laat de Gemeente Lopik zien dat het de informatiebeveiliging serieus neemt en het een onderdeel laat zijn van de ambities om informatie van haar inwoners adequaat te beschermen.
Via ENSIA verantwoordt de gemeente zich ook aan de stelselhouders voor o.a. DigiD, WOZ, BAG en SUWI.

#### 3.3.2 Functionaris voor Gegevensbescherming (FG)
De FG is verantwoordelijk voor het intern onafhankelijk toezien op en adviseren van het college van B&W over de juiste en zorgvuldige omgang met persoonsgegevens zoals de AVG voorschrijft. De FG brengt een jaarverslag uit waarin de bevindingen en aanbevelingen zijn vastgelegd.

## 4. Vaststelling

*Vastgesteld in de vergadering van 19 december 2023.*

*de gemeentesecretaris,*
*drs. F. Jonker*

*de burgemeester,*
*dr. L.J. de Graaf*