College van burgemeester en wethouders

GOEDGEKEURD

Vergadering van 16 juli 2024

Concernstaf & Interne controle - Concernstaf

---

9 **2024_B&W_00547** **Rapport Functionaris gegevensbescherming (FG) Toezicht Algemene Verordening Gegevensbescherming en Wet politiegegevens 2023 - informeren**

Samenstelling:

Aanwezig:

Rob Bats, burgemeester en voorzitter; M. Smit, wethouder; T. Jongman, wethouder; B. Harmsma, wethouder; M. Scheringa, wethouder; D.P. Eikenaar, plv. gemeentesecretaris

Samenvatting

De Functionaris gegevensbescherming (FG) rapporteert in dit verslag over het uitgevoerde toezicht op de naleving van de Algemene Verordening Gegevensbescherming (AVG) en Wet politiegegevens (Wpg) in 2023. Omdat zowel het college als de gemeenteraad verwerkingsverantwoordelijke zijn voor de verwerkingen van persoonsgegevens, wordt dit verslag ook ter kennisneming aan de raad voorgelegd. Op een aantal essentiële processen scoort de gemeente Steenwijkerland goed. Er zijn ook zaken om aan te pakken. Daarvoor doet de FG acht aanbevelingen. Deze zijn aan de directie en de teamleiders voorgelegd en worden of zijn al opgepakt.

Informatienota

Inleiding

In dit rapport beoordeelt de FG als onafhankelijk toezichthouder in hoeverre de gemeente als verwerkingsverantwoordelijke aan de verplichtingen in het kader van de AVG en Wpg voldoet. De Functionaris Gegevensbescherming (FG) adviseert daarbij over een juiste toepassing en doet daarvoor aanbevelingen.

Kernboodschap

De FG geeft acht aanbevelingen. Deze zijn voorgelegd aan de directie en de teamleiders. Die herkennen deze. Ze worden opgepakt of zijn al in uitvoering.

De aanbevelingen gaan over:

1. Privacy voor personeel en sollicitanten
2. Het register van verwerkingen.
3. Reageren op de door het DT onderschreven aanbevelingen in de FG-jaarrapportage 2022
4. Verder voldoen aan Wpg-vereisten en het inbedden van de Wpg-verantwoordelijkheden in de organisatie

5. Het gebruiken van een privacymanagementsysteem
6. Blijven investeren in kennis en trainingen over het privacyveilig gebruik van applicaties.
7. Het doen van Data Protection Impact Assessments (DPIA's)
8. Veilig gebruik van Articifical Intelligence (AI) en algoritmes.

Consequenties voor de gemeente
Het rapport geeft inzicht in de wijze waarop de gemeente Steenwijkerland volgens de Functionaris gegevensbescherming omgaat met de verplichtingen uit de Algemene Verordening Gegevensbescherming (AVG) en Wet politiegegevens (Wpg)

Communicatie
Het rapport en de aanbevelingen zijn intern besproken met de teamleiders en de directie. De aanbevelingen worden door hen herkend en opgepakt in 2024.

Vervolg
De FG zal in 2025 / 2026 de voortgang van de aanbevelingen uit het rapport toetsen en daarover zowel het college als de raad informeren.

Besluit

In te stemmen met de informatienota over het verslag en de aanbevelingen van de Functionaris gegevensbescherming (FG).

Bijlagen

1. Rapport Toezicht FG 2023.BenW_Raad.pdf

Rapport Functionaris gegevensbescherming (FG) Toezicht Algemene Verordening Gegevensbescherming en Wet politiegegevens 2023

V_20240706

Inleiding
De Functionaris gegevensbescherming (FG) rapporteert in dit verslag de gemeente over het uitgevoerde toezicht op de naleving van de Algemene Verordening Gegevensbescherming (AVG) en de Wet politiegegevens (Wpg). De FG is per juni 2023 voor de Wpg benoemd als FG. Naast het toezicht (H1, H2 en H3)heeft de FG geadviseerd over o.a. privacyklachten en -vragen (H4), rechten van betrokkenen (H5) ,datalekken (H6), Data protection Impact Assessments (DPIA's, H7) en toepassing van Artificial Intelligence en algoritmes (H8).

De bestuursorganen van de gemeente zijn wettelijk eindverantwoordelijk voor de verwerkingen van persoonsgegevens die door of namens hen meestal als wettelijke taak worden uitgevoerd. Daarnaast is de publiekrechtelijke rechtspersoon de gemeente in bepaalde gevallen verwerkingsverantwoordelijke. De burgemeester is verantwoordelijk voor de verwerkingen die te maken hebben met zijn veiligheidstaken. De gemeenteraad is verantwoordelijk voor de verwerkingen binnen de griffie en door de raad ingestelde commissies. De publiekrechtelijke rechtspersoon is verantwoordelijk voor onder andere de verwerking van personeelsdossiers. Het college van burgemeester en wethouders is verantwoordelijk voor alle overige gegevensverwerkingen binnen de gemeente en daarmee voor het leeuwendeel van de gemeentelijke verwerkingen.
Wanneer wordt gesproken over de "verwerkingsverantwoordelijke" in de zin van de AVG, wordt bij gemeenten in de regel het college van burgemeester en wethouders bedoeld. Voor de Wpg is dat de gemeente als publiekrechtelijke rechtspersoon, als de werkgever van de Boa's. Deze verantwoordelijkheden brengen verplichtingen met zich mee. In dit rapport beoordeelt de FG als onafhankelijk toezichthouder in hoeverre de gemeente als verwerkingsverantwoordelijke aan de verplichtingen in het kader van de AVG en Wpg voldoet.[1] De Functionaris Gegevensbescherming (FG) adviseert daarbij – gevraagd en ongevraagd - over een juiste toepassing.[2]

Samenvatting en conclusie
Op de volgende voor de AVG essentiële processen scoort de gemeente Steenwijkerland naar het oordeel van de FG goed:

- AVG-bewustwording en informatie
- melden en afdoen van datalekken
- de organisatorische inbedding (H3):
    - de verantwoordelijkheden binnen de organisatie bij de leidinggevenden,
    - de ondersteuning van de leidinggevenden door de I-adviseurs
    - de taken van de Privacy Officer, Chief Information Security Officer en Functionaris gegevensbescherming zijn beschreven en ingevuld
- het uitvoeren van de rechten van betrokkenen
- het afsluiten van verwerkersovereenkomsten
- Er is beleid vastgesteld dat wordt uitgewerkt in een jaarplan en een jaarrapportage

Een aantal processen en onderdelen zal de gemeente Steenwijkerland verder moeten uitwerken om voldoende compliance te realiseren. Dat is voor:

1. Reageren op de aanbevelingen FG-onderzoek privacy voor personeel en sollicitanten

[1] Artikel 39, lid 1 onder b AVG en artikel 36, lid 3 en 4 Wpg
[2] Artikel 39, lid 1, onder a AVG en artikel 36, lid 3 onder b Wpg

2. Het register van verwerkingen. (H1 onder 4)
3. Uitvoeren van of reageren op de door het DT onderschreven aanbevelingen in de FG-jaarrapportage 2022 (H1 onder 6 en H5)
4. Verder voldoen aan Wpg-vereisten en het inbedden van de Wpg-verantwoordelijkheden in de organisatie (H2)
5. Het gebruiken van een privacymanagementsysteem (H3)
6. Blijf investeren in kennis en trainingen over het gebruik van applicaties. (H6)
7. Data Protection Impact Assessments (DPIA's): De FG vraagt de organisatie om haar vooraf te informeren over nieuwe of wijzigingen in risicovolle verwerkingen met persoonsgegevens en adviseert de organisatie meer bekendheid te geven aan DPIA's en de manier waarop deze moeten worden gedaan. (H7)
8. Veilig gebruik van Articifical Intelligence (AI) en algoritmes. (H8)

Het rapport en de acht aanbevelingen van de FG zijn voorgelegd aan de directie en de betrokken teamleiders. De aanbevelingen worden door hen herkend. Sommige zijn al opgepakt en alle andere krijgen in 2024 een vervolg.

Inhoud

1. Toezicht 2023
2. De Wet Politiegegevens (Wpg)
3. Organisatorische inbedding privacy
4. Klacht en vragen inwoners
5. Rechten van betrokkenen
6. Datalekken
7. Data Protection Impact Assessments (DPIA)
8. Artificial intelligence en algoritmes

1. Toezicht 2023

In 2023 is een FG-toezichtsplan opgesteld en uitgevoerd.

1. Onderzoek privacy voor het personeel en sollicitanten: In het eerste kwartaal van 2024 is het FG-onderzoek naar de wijze waarop wordt omgegaan met persoonsgegevens van medewerkers en sollicitanten afgerond en aangeboden aan de teamleider Organisatieadvies.

Aanbeveling 1: De FG adviseert binnen de applicatie het aantal medewerkers dat toegang heeft tot persoonsgegevens, zoals het verslag van het goede gesprek, verder te beperken en om buiten deze applicatie geen persoonsgegevens van sollicitanten en personeelsleden te verwerken, dus niet in Outlook, IBabs, One-Drive en WhatsApp. Ook is het advies de vernietigingsprocedure tijdig uit te voeren en sollicitanten op hun AVG-rechten te wijzen.

2. Onderzoek evaluatie DPIA Cameratoezicht bodycam: het onderzoek is eind 2023 gestart en tijdens het eerste interview zijn de eerste bevindingen gedeeld. Door afwezigheid van de betrokken medewerker is de voortgang gestokt. Verdere uitwerking volgt in 2024.
3. De FG heeft in 2023 advies gegeven over drie Data protection impact assessements (DPIA's) die aan de FG zijn voorgelegd over de processen BOA domeinen I, II en III (openbare orde; milieu, welzijn en infrastructuur; onderwijs (leerplicht)). Zie voor de bevindingen en voortgang H7.
4. Register van verwerkingen: Er is een Register van verwerkingen gemaakt binnen de applicatie I-Navigator van het Document Structuurplan (DSP). In het DSP zijn alle gemeentelijke

processen beschreven. Dit register werkbaar, inzichtelijk, beheersbaar en actueel houden voor de hele organisatie is de volgende uitdaging. Daar gaat de FG op toezien. De FG raadt aan om het register naast intern ook extern toegankelijk respectievelijk zichtbaar te maken. Zo kunnen betrokkenen kennisnemen van de verwerkingen die de gemeente heeft. Dat stelt hen in staat daar regie op te nemen en hun rechten als betrokkenen uit te oefenen.

Aanbeveling 2: De FG adviseert het register van verwerkingen intern toegankelijk/zichtbaar te maken en extern te publiceren, bijvoorbeeld op de gemeentelijke website.

5. Datalekprocedure: conform het processchema dat eind 2022 is vastgesteld voor de datalekprocedure wordt een gemeld datalek als eerste beoordeeld door de Chief Information Security Officer (CISO) en de privacy officer (PO). De FG ontvangt hun beoordelingsformulier over de te nemen en genomen maatregelen en het melden bij de Autoriteit Persoonsgegevens en betrokkenen. De FG stuurt dit samen met een advies naar de betrokken leidinggevende(n) en medewerker(s). De leidinggevende is verantwoordelijk voor het afdoen van een datalek, het treffen van maatregelen en het informeren van betrokkenen en het eventueel melden bij de Autoriteit persoonsgegevens. De FG constateert dat dit proces door de betrokkenen conform het processchema doorlopen wordt en is hier tevreden over.
6. De adviezen van de FG in 2023[3] om een privacymanagementtool te gebruiken (zie ook H3), een privacyverklaring voor processen jeugd te publiceren en in de werkprocessen en instructies bij de processen jeugd vast te leggen dat betrokken tijdig worden geïnformeerd over het vastleggen van persoonsgegevens en hun rechten (Zie ook H5) zijn overgenomen door het DT en moeten nog worden uitgevoerd.

Aanbeveling 3: Uitvoeren van de door het DT onderschreven aanbevelingen in de FG-jaarrapportage 2022, zoals hierboven beschreven.

2. De Wet Politiegegevens (Wpg)

Per 1 januari 2019 is de Wet Politiegegevens (Wpg) in werking getreden. In de Wpg is voor de verwerkingsverantwoordelijke de verplichting opgenomen om elk jaar een interne audit te doen en één keer in de vier jaar een externe audit,[4] Aan de hand hiervan kan worden vastgesteld of de gemeente bij de verwerkingen onder Wpg voldoet aan de wettelijke eisen en kan waar nodig worden bijgestuurd. De teamleiders van de organisatieonderdelen waar de boa's werkzaam zijn, zijn hiervoor verantwoordelijk.

In 2022 heeft de gemeente Steenwijkerland door een externe auditor de Wpg-audit laten doen en daarop is een verbeterplan gemaakt. Dit is uitgevoerd en inmiddels geaudit. In 2023 is de FG ook aangewezen als FG voor de Wpg en zijn de DPIA's BOA domeinen I, II en II aan de FG ter advisering voorgelegd. Deze DPIA's zijn door de FG als ontoereikend beoordeeld, omdat de risicoanalyse ontbreekt.

Aanbeveling 4: Verder werken aan het voldoen aan de Wpg vereisten en het inbedden van de Wpg-verantwoordelijkheden in de organisatie.

3. Organisatorische inbedding privacy

Voor een goede en juiste uitvoering van de AVG is het van belang dat een ieder binnen de organisatie op de hoogte is van wie welke taken, verantwoordelijkheden en bevoegdheden heeft. In Steenwijkerland is eind 2022 de organisatorische inbedding van privacy en informatieveiligheid

[3] Rapport FG 2022, DT 10 februari 2022, B&W 1 maart 2022
[4] art. 33 Wpg: audits

binnen de gemeente vastgelegd in een privacygovernance. Elke leidinggevende (eerste lijn) is verantwoordelijkheid voor het implementeren van privacymaatregelen binnen diens eenheid. Daarbij worden ze ondersteund door I-adviseurs. In de privacygovernance staan ook de taken, verantwoordelijkheden en bevoegdheden binnen het privacyteam. De privacy officers en Chief Information Security Officer (CISO) adviseren de organisatie als de tweede lijn. Zij rapporteren hierover separaat met een jaarplan, auditplan en verslag. De FG is gericht op toezicht in de derde lijn en stelt hiervoor periodiek een toezichtplan en een verslag op.

Om als FG het toezicht optimaal te kunnen doen, is een werkende privacymanagementtool nodig. Deze software genereert een beeld van de status van de processen en activiteiten die AVG- en Wpg-wettelijk vereist zijn. Dat geeft het management en de FG inzicht in de privacy-volwassenheid van de organisatie en draagt bij aan het onderbouwen van keuzes voor het wel of niet accepteren van privacyrisico's en het treffen van maatregelen om te voldoen aan de privacywetgeving. Het DT heeft het advies van de FG om een privacymanagementtool te gebruiken in 2023 overgenomen. Dit is nog niet gerealiseerd.

Aanbeveling 5: Een privacymanagementsysteem inrichten en gebruiken

4. Klachten, vragen en contact betrokkenen

De AVG verplicht gemeenten om de contactgegevens van de FG te publiceren zodat betrokkenen contact kunnen opnemen met deze functionaris. In 2023 hebben drie betrokkenen van deze mogelijkheid gebruik gemaakt. Twee privacyklachten zijn tevens datalekken.

- Eén betreft twee verschillende mails over een betrokkene die naar een verkeerde ontvanger zijn gestuurd.
- De tweede is dat een medewerker van de gemeente de naam van betrokkene heeft genoemd in een gesprek met een andere externe. Degene die met betrokkene contact opnam over het datalek was bij het gesprek geweest. De betrokkene voelde zich daardoor niet serieus genomen.

Deze twee klachten en datalekken zijn besproken met betrokkenen en diens leidinggevenden. De gemeente heeft voor de datalekken excuses gemaakt aan de klagers en maatregelen genomen om herhaling te voorkomen.

- De derde klacht betreft de uitnodiging om mee te doen aan een enquête. Deze uitnodiging krijgen bellers naar het Klantcontactcentrum (KCC) via een sms-bericht na afloop van hun telefoongesprek. Het sms-bericht wordt verstuurd door een externe dienstverlener. Deze werkwijze waarbij een externe dienstverlener het telefoonnummer van de beller krijgt, wordt niet van tevoren gemeld aan de bellers en er is geen vooraf opt-in -keuze[5]. Betrokkene was het daarmee niet eens en wilde weten hoelang haar telefoonnummer bij de externe dienstverlener bewaard blijft. Hoe dit werkt, is besproken met het team Ontvangst en door de FG met de klager. De FG heeft het team Ontvangst geadviseerd om betrokkenen hierover actief te informeren. Dat kan voor, tijdens of na het telefoongesprek, i.i.g. voordat de sms wordt verstuurd . Nog beter is om een opt-in aan te bieden. Bij de gemeente zijn hier niet eerder klachten over geweest en daarom is besloten dit niet te doen, ook omdat in de privacyverklaring van de gemeente staat dat persoonsgegevens worden verwerkt voor het uitvoeren van tevredenheidsonderzoeken om onze dienstverlening te kunnen verbeteren.[6] Hiermee zijn de klachten van de klagers naar hun tevredenheid afgedaan.

Verder is FG contactpersoon geweest voor betrokkenen die getroffen zijn door een datalek veroorzaakt en gemeld door een externe dienstverlener die persoonsgegevens voor de gemeente

[5] Opt in – keuze houdt in dat de betrokkene van te voren kan aangeven wel of geen prijs te stellen op een enquête. Hiermee houdt betrokkene regie of deze wel of niet benaderd wordt voor een enquête en of diens gegevens mogen worden doorgezet naar de enquêteur. In het geval van bijvoorbeeld direct marketing is (vrijblijvende) opt in een privacy-by-default-voorwaarde.

[6] Privacyverklaring gemeente Steenwijkerland - Gemeente Steenwijkerland

verwerkt. Betrokkenen zijn hierover door de gemeente goed geïnformeerd en de procedure is naar tevredenheid van betrokkenen afgesloten.

5. Rechten van betrokkenen

De AVG bepaalt niet alleen de plichten van degenen die persoonsgegevens verwerken, maar bepaalt ook de rechten van de personen van wie gegevens worden verwerkt.[7] Ook de Wpg regelt dat.[8] Deze rechten worden de rechten van betrokkenen genoemd. Dat is om betrokkenen regie of controle te geven over de verwerking van diens persoonsgegevens. De gemeente moet deze verzoeken als verwerkingsverantwoordelijke afhandelen. Er is in 2023 één AVG-inzage verzoek geweest en afgehandeld. Dit inzageverzoek is naar veel Nederlandse gemeenten gestuurd en gaf veel onrust, omdat de gevraagde inzagegegevens en contactgegevens niet duidelijk waren.

De FG heeft in 2022 de organisatie geadviseerd over transparantie bij jeugdprocessen. Om beter te voldoen aan de AVG-beginselen informatieplicht en transparantie adviseert de FG een privacyverklaring over gegevensverwerkingen in jeugdprocessen te publiceren. Een tweede advies is om in de werkprocessen/werkinstructie vast te leggen hoe en dat betrokkenen tijdig worden geïnformeerd over het verwerken van persoonsgegevens en hun rechten. Deze aanbevelingen zijn overgenomen en worden in 2024 uitgevoerd. (Zie aanbeveling 4.)

6. Datalekken

Er zijn in 2023 22 datalekken intern gemeld en behandeld. Een als risicovol beoordeelde datalek is gemeld aan de Autoriteit persoonsgegevens (AP). Een ander datalek leek bij het begin ervan risicovol en is daarom gemeld bij de AP, maar de melding is ingetrokken toen uit nader onderzoek bleek dat er geen persoonsgegevens zijn gelekt. Zeven datalekken zijn gemeld aan de betrokkenen.

Dit zijn tien meldingen van datalekken meer dan vorig jaar. Deze stijging betekent zeker niet dat de organisatie onveiliger is gaan werken. Meer waarschijnlijk is dat de medewerkers meer bewust zijn van wat een datalek is en hoe je deze moet melden. Dat is dus een goede ontwikkeling.

De meeste datalekken zijn veroorzaakt door verkeerde adressering per mail (11) en post (4).

Ook worden datalekken veroorzaakt door onjuist gebruik of een (tijdelijke) onjuiste werking van een applicatie, zoals

1. Medewerkers die met meerdere zaken tegelijk bezig zijn in het zaaksysteem en dan per abuis mailen naar de betrokkene bij de andere zaak;
2. Een medewerker die sjablonen uit de verkeerde applicatie gebruikt;
3. Medewerkers die per abuis een verkeerde optie aanvinken waardoor de gegevens voor meer medewerkers dan toegestaan, beschikbaar zijn;
4. Medewerkers die via Outlook een mail verzenden naar de privémail of op de eigen schijf (in plaats van de HR-applicatie) gegevens over (ziekte van) een medewerker vastleggen.

Twee datalekken zijn veroorzaakt door per abuis in zakelijke gesprekken mededelingen te doen over een externe. Dit is door de leidinggevenden met de betrokken medewerkers en in de teams besproken.

Eén datalek werd veroorzaakt door een hack bij een serviceleverancier waardoor kortstondig ongeautoriseerde toegang is geweest tot een applicatie met gegevens van (oud)medewerkers. Deze zijn door de gemeente geïnformeerd. Uit nader onderzoek is gebleken dat er geen persoonsgegevens zijn buitgemaakt. Daarop is de melding bij de Autoriteit Persoonsgegevens ingetrokken.

[7] artt 13 tot en met 20 AVG

[8] artt 24 tot en met 28 Wpg

Veilig werken in applicaties staat en valt bij de bekendheid ervan bij de medewerkers. Bij applicaties die complex en ingewikkeld zijn, kunnen datalekken ontstaan door onjuist gebruik ervan of door het vermijden ervan. Mogelijk worden er dan applicaties gebruikt voor verwerken van persoonsgegevens die daarvoor niet bedoeld zijn. In 2023 zijn voor Teams en Zaaksysteem trainingen aangeboden. Dat draagt bij aan een privacyveilig gebruik. Het advies is om deze trainingen regelmatig te herhalen zodat ook nieuwe medewerkers en medewerkers die herhaling willen, de kennis kunnen opdoen.

Aanbeveling 6: Blijf investeren in kennis en trainingen over het privacyveilig gebruik van applicaties.

7. Data protection Impact Assessments (DPIA's)

Er zijn in 2023 drie DPIA's aan de FG voorgelegd. Die DPIA's gaan over de werkprocessen van de BOA's domeinen I, II en III. De FG heeft geconstateerd dat deze niet aan de inhoudelijke eisen van de AVG voldoen. Drie DPIA's zou betekenen dat er in de gemeente Steenwijkerland in 2023 verder geen nieuwe verwerkingen met persoonsgegevens zijn gestart en of (technologische) wijzigingen in risicovolle verwerkingen zijn geweest. Het lijkt dat er te weinig uitvoering is gegeven aan DPIA's in 2023.
Voor het voldoen aan de DPIA-verplichting[9], moet de gemeente blijven monitoren of er veranderingen zijn in

- Gegevensverwerkingen
- De risico's van een verwerking
- De context van een verwerking

Aanbeveling 7: De FG vraagt de organisatie om tijdig te inventariseren en de FG te informeren over nieuwe of wijzigingen in verwerkingen van persoonsgegevens, zodat het doen van DPIA's beter ingebed wordt.

8. Artificial intelligence en algoritmes

De FG heeft in de Securityboard aandacht gevraagd voor de toenemende rol van Artificial Intelligence (AI), (zelflerende) algoritmes en de verplichtingen vanuit de AI die in 2026 in werking treedt.[10] Het advies is om de komende twee jaar te gebruiken om tijdig en gestructureerd met Artificial Intelligence e om te gaan en om in de toekomst aan de vereisten uit wet- en regelgeving te kunnen blijven voldoen.

De gemeente onderzoekt het gebruik van AI-technologie als Chat-Gpt en Co-Pilot. In dit digitale tijdperk is het van belang om AI-tools te benutten, maar daarbij moeten ethische en privacy kwesties wel worden meegenomen. De FG constateert dat de organisatie nog geen inventarisatie heeft van de nu gebruikte AI en algoritmes en nog geen (risicovolle) algoritmes heeft gepubliceerd in het Algoritmeregister. De FG adviseert dat wel te gaan doen. Transparantie hierover vergroot immers het vertrouwen in de gemeentelijke dienstverlening. Verder adviseert de FG bij de inzet van AI de volgende stappen te nemen om ethische, privacy- en informatiebeveiligingsriscio's te limiteren:

1. Transparantie en uitlegbaarheid: AI-systemen moeten transparant zijn in hun besluitvorming en kunnen uitleggen hoe ze werken (de black box moet inzichtelijk zijn)

[9] Art 35 AVG

[10] Er zijn onacceptabele AI's (in strijd met mensenrechten en mogen daarom niet, bijvoorbeeld prediciting policy en emotieherkenning op de werkvloer), hoogrisicovolle AI's (zelflerend en tot rechtsgeldige besluiten leidend, die mogen onder voorschriften) en laagrisicovolle AI's (een chatbox).

2. Privacy en gegevensbescherming: cruciaal is het beschermen van persoonlijke gegevens en voldoen aan privacywetgeving (geen tot personen herleidbare gegevens gebruiken, want het risico is dat alles wordt bewaard en verwerkt door de AI-systemen)
3. Bias en discriminatie: vermijden van inherente vooroordelen en zorgen voor eerlijke resultaten zonder discriminatie op basis van demografische kenmerken
4. Verantwoordelijkheid en aansprakelijkheid: duidelijkheid over wie verantwoordelijk is voor de beslissingen van AI-systemen en hoe eventuele fouten worden behandeld (verplicht bij hoogrisicovolle AI)
5. Veiligheid en beveiliging: beschermen van AI-systemen tegen aanvallen om misbruik en schade te voorkomen

Gebruikers moeten goed geïnformeerd zijn over de technologie die ze gebruiken. De FG adviseert de verantwoordelijkheid voor het gebruik van AI en algoritmes binnen de organisatieonderdelen te borgen en om richtlijnen en proefprojecten te starten om de organisatie en medewerkers voor te bereiden op veilig gebruik van AI. Een AI-officer, een ethisch officer en een ethische commissie zou hierbij kunnen ondersteunen.

Aanbeveling 8:

- *Inventariseer de artificial intelligence (AI) en algoritmes die gebruikt worden door de gemeente Steenwijkerland*
- *Classificeer deze zoals vastgesteld in de AI-Act op risiconiveaus en bijbehorende voorschriften*
- *Publiceer de (hoog-)risicovolle in het Algoritmeregister*
- *Beleg de verantwoordelijkheid voor het gebruik van AI bestuurlijk en ambtelijk (governance)*
- *Stel beleid en richtlijnen vast voor het gebruik van AI en algoritmes en let daarbij op de ethische en privacy- en informatiebeveiligingsrisico's. Sommige gemeenten hebben daarvoor een ethische commissie, een AI-adviseur en of een ethisch officer.*
- *Voer een impact assessment (Fundamental rights impact assessment ofwel mensenrechtentoets) uit op de inzet van AI en algoritmes en neem dit als voorwaarde mee bij inkoop.*