

## Privacybeleid gemeente Goes

### 1. Inleiding

De gemeente werkt met (persoons)gegevens van burgers, ondernemers, medewerkers en (keten)partners. Deze gegevens verzamelt de gemeente om de gemeentelijke wettelijke taken goed uit te kunnen voeren. Denk hierbij aan taken in het sociaal domein, openbare orde en veiligheidsdomein of voor burgerzaken. Om deze taken goed te volbrengen is het noodzakelijk dat de gemeente persoonsgegevens verwerkt. De burger moet erop kunnen vertrouwen dat de gemeente zorgvuldig en veilig met deze persoonsgegevens omgaat.

Nieuwe technologische ontwikkelingen, innovatieve voorzieningen, globalisering en een overheid die steeds vaker gebruik maakt van digitale systemen maakt het zorgvuldig omgaan met persoonsgegevens steeds complexer en noodzakelijker. De gemeente 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 (hierna te noemen: AVG). Dit beleid is vastgesteld door het college als bestuurlijk eindverantwoordelijke voor de gemeentelijke gegevensverwerking. Het beleid wordt tenminste eens per drie jaar beoordeeld en zo nodig herzien.

### 2. Doel

Met dit privacybeleid geeft de gemeente een kader voor het verantwoord omgaan met persoonsgegevens en het waarborgen van de persoonlijke levenssfeer van de personen waarvan de gemeente persoonsgegevens verwerkt (of laat verwerken). Daarnaast beoogt dit privacybeleid taken en verantwoordelijkheden op het gebied van de bescherming van persoonsgegevens helder af te bakenen.

De verdere uitwerking van dit beleid is - waar relevant - vastgelegd in de operationele documenten binnen de gemeente, zoals handreikingen, concrete werkprocedures of werkafspraken voor algemene onderwerpen zoals datalekken, maar ook domeinspecifieke onderwerpen als gegevensdeling voor de uitvoering van de Jeugdwet of de Wet Maatschappelijke Ondersteuning.

Naast dit door het college vastgestelde privacybeleid is een informatiebeveiligingsbeleid vastgesteld. Hierin zijn maatregelen opgenomen om de beschikbaarheid, integriteit en vertrouwelijkheid van (persoons)gegevens te garanderen. Informatiebeveiliging is een randvoorwaarde voor de bescherming van persoonsgegevens. Het gemeentelijke privacybeleid kan daarom niet los worden gezien van het gemeentelijke informatiebeveiligingsbeleid.

Iedereen werkzaam binnen de gemeente is verantwoordelijk voor het verantwoord omgaan met persoonsgegevens. De gemeente verlangt van al haar medewerkers en alle personen die werkzaam zijn voor de gemeente dat de voorschriften van dit privacybeleid worden opgevolgd en actief worden uitgedragen.

### 3. Reikwijdte

De gemeente verzamelt en gebruikt persoonsgegevens van inwoners, leveranciers en medewerkers en andere natuurlijke personen (hierna te noemen: betrokkenen). Dit privacybeleid is, met uitzondering van werkingen op grond van de Wet politiegegevens, van toepassing op alle verwerkingen van persoonsgegevens door of namens de gemeente, waaronder:

1. De verwerking van persoonsgegevens binnen de bedrijfsprocessen van de gemeente;
2. De verwerking van persoonsgegevens die is uitbesteed, of op een andere manier is georganiseerd, zoals deelname van de gemeente aan een rechtspersoon die voor de gemeente bepaalde diensten verricht;
3. De gegevensuitwisseling met derde partijen zoals bij samenwerkingsverbanden of leveranciers.

Voor alle verwerkingen waarop de Wet politiegegevens ziet, geldt een afzonderlijk beleid.

### 4. Principes voor de verwerking van persoonsgegevens

De AVG is gebaseerd op een aantal principes voor de verwerking van persoonsgegevens. De gemeente onderschrijft deze principes en stelt zich ten doel persoonsgegevens slechts te verwerken in overeenstemming met deze principes.

### **Rechtmatige grondslag**

Persoonsgegevens worden door de gemeente slechts verwerkt in overeenstemming met de wet en op een behoorlijke en zorgvuldige wijze. Dit betekent onder meer dat verwerkingen alleen plaatsvinden indien hiervoor een rechtmatige verwerkingsgrondslag bestaat. Veelal vloeit de grondslag voor een verwerking bij een gemeente voort uit een wet (wettelijke verplichting) of een publiekrechtelijke taak.

### **Welbepaalde doeleinden**

De gemeente verwerkt persoonsgegevens voor zeer uiteenlopende doeleinden. Zonder doel mogen persoonsgegevens niet worden verwerkt. De verwerking van persoonsgegevens vindt plaats op een wijze die noodzakelijk is om de doeleinden te bereiken waarvoor de gegevens zijn verkregen. Dit betekent dat de gemeente alleen die persoonsgegevens verwerkt die noodzakelijk zijn om het doel te bereiken (ter zake dienend). De gemeente ziet af van de verwerking als het doel op een andere – minder ingrijpende – wijze kan worden bereikt, bijvoorbeeld door minder of geen persoonsgegevens te verwerken.

### **Verdere verwerking**

Persoonsgegevens kunnen in bepaalde gevallen worden verwerkt voor andere doelen dan waarvoor ze in eerste instantie zijn verzameld. Daarbij geldt onder andere dat de twee doelen aan elkaar verwant moeten zijn, er zich geen nadelige effecten voor de betrokkenen voordoen, dan wel dat hiervoor extra waarborgen zijn getroffen. De gemeente voert, voordat de verwerking start, een toets uit om te bepalen of de gegevens voor andere doelen mogen worden gebruikt op grond van de wet- en regelgeving.

### **Minimale gegevensverwerking**

Gegevens mogen alleen worden verwerkt als dit in verhouding staat tot het doel. Als het doel waarvoor persoonsgegevens worden verwerkt, zonder of met minder persoonsgegevens kan worden bereikt, dan kiest de gemeente bij voorkeur voor die mogelijkheid. Ook als het doel waarvoor persoonsgegevens worden verwerkt op een wijze kan worden verwezenlijkt die minder inbreuk maakt op de privacy van de betrokkene, dan kiest de gemeente bij voorkeur voor die mogelijkheid.

### **Juiste en actuele gegevens**

De gemeente zorgt ervoor dat alleen persoonsgegevens worden verwerkt die juist en actueel zijn gelet op het doel waarvoor zij verzameld zijn of vervolgens worden verwerkt. De gemeente neemt redelijke maatregelen om persoonsgegevens juist en actueel te houden, onjuiste persoonsgegevens te actualiseren, te rectificeren en/of te wissen.

### **Gegevens worden op tijd vernietigd**

De gemeente stelt de bewaartermijn van een verwerking vast aan de hand van wettelijke bepalingen en de selectielijsten. Gemeenten hebben op grond van de Archiefwet 1995 onder andere de plicht om zogenaamde selectielijsten op te stellen. Deze selectielijsten bepalen voor een selectie van documenten hoelang deze moeten worden bewaard. Alleen als de bewaartermijn niet op basis van wettelijke bepalingen of de selectielijsten kan worden vastgesteld, stelt de gemeente de bewaar-termijn vast op basis van noodzakelijkheid. Persoonsgegevens mogen dan niet langer worden bewaard dan noodzakelijk. De gemeente bewaart gegevens alleen langer als deze geanonimiseerd worden, zodat directe of indirecte identificatie van een persoon niet meer mogelijk is.

### **Integriteit en vertrouwelijkheid**

De gemeente neemt passende technische en organisatorische maatregelen om de persoonsgegevens, met name bijzondere persoonsgegevens, te beschermen tegen misbruik en onrechtmatige of ongeautoriseerde verwerking. De gemeente handelt hierbij in overeenstemming met het informatiebeveiligingsbeleid. Het informatiebeveiligingsbeleid verplicht de gemeente om informatie te beveiligen tegen ongeautoriseerd gebruik, vernietiging (per ongeluk of onrechtmatig), verlies of vervalsing, onbevoegde bekendmaking of toegang en alle andere onrechtmatige manieren van verwerking.

### **Privacy by Default en Privacy by Design**

De gemeente houdt bij de ontwikkeling van nieuwe diensten, systemen of processen rekening met aspecten van privacy en gegevensbescherming om zo te komen tot een zo optimaal mogelijke bescherming van Persoonsgegevens. Dit uitgangspunt wordt *Privacy by Design* genoemd. De gemeente draagt er zorg voor dat concrete maatregelen zoveel mogelijk doorgevoerd worden in het ontwerp. Daarbij neemt de gemeente *Privacy by Default* als uitgangspunt: de standaardinstellingen zijn altijd zo privacy-vriendelijk mogelijk.

### **Toegang tot gegevens**

Uitsluitend geautoriseerde gebruikers zijn bevoegd tot onder meer het invoeren, rechtstreeks raadplegen, wijzigen en verwijderen van persoonsgegevens voor zover aan hen hiervoor bevoegdheden zijn toegekend. Deze bevoegdheden worden verleend op grond van het binnen de gemeente geldend beleid voor

toegang tot gegevens, waaronder het informatiebeveiligingsbeleid. Het beheer van bevoegdheden wordt periodiek gecontroleerd. De gemeente hanteert daarnaast specifieke oplossingen en toepassingen, waaronder het bijhouden van loggegevens, om ongeautoriseerde toegang tot en niet toegestane verwerkingen van persoonsgegevens zo veel mogelijk te voorkomen en aan te pakken.

#### **Inbreuk in verband met persoonsgegevens**

Bij toegang tot, verlies of wijziging van persoonsgegevens bij de gemeente, zonder dat dit de bedoeling is, is er sprake van een datalek. Dat moet, afhankelijk van het risico, worden gemeld bij de toezichthouder (de Autoriteit Persoonsgegevens) en soms bij de getroffen betrokkenen. De gemeente registreert datalekken, zet de bevindingen om in verbeterpunten en ziet toe op de opvolging hiervan. Nadere regels ten aanzien van het vaststellen, melden en afhandelen van datalekken zijn opgenomen in de procedure meldplicht datalekken van de gemeente Goes.

#### **Samenwerking**

De gemeente schakelt soms derden in om persoonsgegevens in opdracht van haar te verwerken. Deze derden worden verwerkers genoemd. Ook een verwerker moet zich houden aan de privacyregelgeving en aan het privacybeleid van de gemeente. De AVG verplicht gemeenten tot het maken van contractuele afspraken met verwerkers, zogenaamde verwerkersovereenkomsten.

#### **Samenwerkingsverbanden**

Verder kan het voorkomen dat de gemeente samenwerkt met andere (overheids)organisaties om een taak van algemeen belang uit te voeren. In die gevallen kan sprake zijn van meerdere verwerkersverantwoordelijken (gezamenlijk of individueel). De gemeente maakt met deze organisaties afspraken over de wijze waarop persoonsgegevens worden verwerkt. Derden waarborgen een beschermingsniveau dat gelijk is aan dat van de gemeente.

#### **Doorgifte buiten de EER**

Doorgifte van persoonsgegevens aan landen buiten de Europese Economische Ruimte (EER) of een internationale organisatie, geschiedt alleen in overeenstemming met de relevante bepalingen in toepasselijke wet- en regelgeving en dit privacybeleid.

#### **Transparantie**

De gemeente informeert de betrokkenen tijdig, op een zo eenvoudig mogelijke, begrijpelijke en toegankelijke wijze over het feit dat zij persoonsgegevens verwerkt, op welke wijze en voor welke doeleinden. De betrokkene wordt op heldere en laagdrempelige wijze geïnformeerd over zijn rechten en de wijze waarop hij deze kan uitoefenen. Alleen indien de wet anders bepaalt, wijkt de gemeente van deze informatieplicht af.

#### **Rechten van betrokkenen**

Iedereen heeft het recht om te vernemen welke persoonsgegevens de gemeente over hem/haar heeft verzameld en waarvoor deze worden gebruikt. Betrokkenen hebben de mogelijkheid om hun rechten uit hoofdstuk III van de AVG uit te oefenen, te weten het recht van inzage, recht op rectificatie, recht op verwijdering, recht op bezwaar, recht op beperking en recht op overdraagbaarheid. De rechten van betrokkenen staan op de website van de gemeente en daarop staat een digitaal formulier om een verzoek in te dienen ten aanzien van deze rechten.

#### **Geschillenbeslechting**

Indien de betrokkene van mening is dat de gemeente niet op een juiste wijze met zijn persoonsgegevens is omgegaan, kan hij een klacht indienen door middel van de van toepassing zijnde klachtenprocedure zoals opgenomen in de privacyverklaring op de website. De betrokkene heeft ook het recht een klacht in te dienen bij de Autoriteit Persoonsgegevens, met betrekking tot de naleving van wet- en regelgeving op het gebied van de bescherming van persoonsgegevens.

#### **Verantwoording**

Onder de bestuurlijke verantwoordelijkheid van het gemeentebestuur vindt een groot aantal verwerkingen van persoonsgegevens plaats. Daar vindt extern en intern toezicht op plaats. De Autoriteit Persoonsgegevens (AP) houdt toezicht op de naleving van de privacyregels in Nederland. Daarnaast beschikt de gemeente over een interne toezichthouder: de Functionaris Gegevensbescherming (FG). De FG ziet erop toe dat de AVG intern wordt nageleefd. De gemeente stelt voldoende middelen ter beschikking aan de FG om het toezicht adequaat uit te kunnen voeren.

#### **Verwerkingsregister**

De gemeente beschikt over een verwerkingsregister, waarin alle verwerkingen van persoonsgegevens gedocumenteerd zijn en inzichtelijk zijn gemaakt.

## DPIA

Als een verwerking mogelijk een hoog risico inhoudt voor de betrokkene, moet de gemeente een beoordeling uitvoeren van het effect van een verwerking van persoonsgegevens. De gemeente voert in dat geval een gegevens effect beoordeling uit (ook wel Data Processing Impact Assessment of DPIA genoemd). Als hieruit blijkt dat er inderdaad hoge risico's zijn verbonden aan de verwerking, moet de gemeente voldoende maatregelen nemen om de risico's te verminderen.

## Functionaris gegevensbescherming (FG)

De gemeente is een overheidsinstantie die structureel en op grote schaal persoonsgegevens verwerkt, waaronder bijzondere persoonsgegevens. De gemeente is daarom verplicht een FG aan te stellen. De FG is de onafhankelijke intern toezichthouder en heeft een adviserende, informerende en toezichthoudende taak. Dit betekent dat de FG toeziet op alle verwerkingen van persoons-gegevens. De FG brengt jaarlijks een verslag uit aan het college van burgemeester en wethouders.

## PDCA Cyclus

De gemeente streeft ernaar om rondom de verwerking van persoonsgegevens in control te zijn en daarover op professionele wijze verantwoording af te leggen. In control betekent in dit verband dat de gemeente weet welke maatregelen genomen zijn ten aanzien van de verwerking van persoons-gegevens dat er een planning is van de maatregelen die nog niet genomen zijn en dat dit geheel verankerd is in een Plan-Do-Check-Act-cyclus. Daarnaast gebruikt de gemeente het borgingsproduct van de VNG als het beoordelingskader voor het waarborgen van privacy compliance binnen de gemeente. Het borgingsproduct is een normenkader wat door de gemeente gebruikt wordt voor het duiden van privacy risico's en de daarbij behorende beheersmaatregelen binnen de gemeente.

## Bewustwording

Beleid en maatregelen zijn niet voldoende om risico's op het terrein van het verwerken van persoonsgegevens uit te sluiten. Het is noodzakelijk om het bewustzijn in de gemeentelijke organisatie voortdurend aan te scherpen, zodat kennis van risico's wordt verhoogd en (veilig en verantwoord) gedrag om persoonsgegevens zorgvuldig te verwerken wordt aangemoedigd. Iedere medewerker wordt geïnformeerd over het zorgvuldig omgaan met persoonsgegevens.

## 5. Rollen en Verantwoordelijken

Het governancemodel van de gemeente biedt een overkoepelende visie en strategie hoe de bescherming van persoonsgegevens effectief belegd wordt binnen de organisatie. Daartoe bevat het een beschrijving van de taken en verantwoordelijkheden van het College van B&W, het managementteam en medewerkers, de Functionaris voor de Gegevensbescherming (FG), de Privacy Officer en de Chief Information Security Officer (CISO).

|   | Verantwoordelijk                        |                                                                                                                                                                                                                                                                                               |
|---|-----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| R | Responsible/ Feitelijk verantwoordelijk | <ul style="list-style-type: none"> <li>Afdelingshoofden en gemeentesecretaris zijn ambtelijk verantwoordelijk.</li> <li>De medewerkers (inclusief inhuur/externen) die persoonsgegevens verwerken</li> </ul>                                                                                  |
| A | Accountable/ Eindverantwoordelijk       | <ul style="list-style-type: none"> <li>Het college is bestuurlijk eindverantwoordelijk</li> </ul>                                                                                                                                                                                             |
| C | Consulted/ Adviserend                   | <ul style="list-style-type: none"> <li>Privacy Officer</li> <li>Chief Information Security Officer</li> <li>Functionaris Gegevensbescherming</li> </ul>                                                                                                                                       |
| I | Informed/ Geïnformeerd                  | <ul style="list-style-type: none"> <li>Gemeenteraad (privacy rechtelijk geen controlerende taak, maar op basis van de Gemeentewet en de decentralisatiewetgeving een bestuurlijke toezichttaak)</li> <li>Functionaris Gegevensbescherming</li> <li>Belanghebbende(n)/Betrokkene(n)</li> </ul> |

## College

Het college is bestuurlijk eindverantwoordelijk voor de naleving van de privacywetgeving binnen de gemeente. Het college heeft de volgende rollen en verantwoordelijkheden:

- Bestuurlijk eindverantwoordelijk voor de naleving van de privacywetgeving binnen de gemeente;

- Stelt het privacybeleid vast;
- Geeft sturing aan privacy beleidsvoering en legt rekenschap af over privacy beleidsvoering aan de Functionaris Gegevensbescherming;
- Evalueert de toepassing en werking van het privacybeleid op basis van de rapportage van Functionaris Gegevensbescherming;
- Bevordert duurzame privacycultuur.

#### **Afdelingshoofden en gemeentesecretaris**

De afdelingshoofden en gemeentesecretaris zijn ambtelijk eindverantwoordelijk voor de naleving van de privacywetgeving binnen de afdeling, alsmede voor de uitvoering van het privacybeleid. De afdelingshoofden en de gemeentesecretaris hebben de volgende rollen en verantwoordelijkheden:

- Ambtelijk eindverantwoordelijk voor de naleving van de privacywetgeving binnen de eigen afdeling;
- Verantwoordelijk voor implementatie en uitvoering van het privacybeleid binnen de eigen afdeling;
- Informeert de FG op welke manier een afdeling voldoet aan de privacywetgeving;
- Verantwoordelijk voor (laten) volgen van trainingen door werknemers binnen de eigen afdeling;
- Verantwoordelijk voor registreren van de gegevensverwerkingen in het verwerkingenregister voor zover dit betrekking heeft op de eigen afdeling;
- Verantwoordelijk voor autorisatie en intrekken van de autorisatie van medewerkers die persoonsgegevens verwerken;
- Aansturen van de Privacy Officer (via afdelingshoofd Concern);
- Bevordert een duurzame privacy cultuur;
- Betrekt PO en/of FG in een vroeg stadium bij nieuwe of gewijzigde verwerkingen van persoonsgegevens.

#### **Functionaris Gegevensbescherming (FG)**

Op basis van de AVG is het aanstellen van een FG verplicht voor de gemeente. De FG is verantwoordelijk voor het toezicht op de naleving van de AVG. De FG heeft een onafhankelijke adviserende en toezicht houdende positie in de organisatie. De FG heeft de volgende rollen en verantwoordelijkheden in de gehele organisatie van de gemeente:

- Interne toezichthouder op de naleving van de AVG namens de Autoriteit Persoonsgegevens;
- Draagt privacybeleid actief uit binnen de gehele gemeente en bevordert een cultuur van duurzame gegevensbescherming;
- Adviseert verwerkingsverantwoordelijken bij privacyklachten en verzoeken van betrokkenen (ombudsfunctie);
- Adviseert verwerkingsverantwoordelijken ten aanzien van het mitigeren van privacy risico's, bijvoorbeeld bij het uitvoeren van DPIA's en hoog-risico dossiers;
- Beschikt over controle- en monitoringbevoegdheden (het recht om interne onderzoeken te laten uitvoeren met toegang tot informatie);
- Rapporteert jaarlijks aan het college van burgemeester en wethouders.

#### **Privacy Officer (PO)**

De PO is het eerste aanspreekpunt voor de gemeente rondom privacy gerelateerde vraagstukken, en heeft een monitorende en ondersteunende functie rondom het naleven en uitvoeren van het privacybeleid. De PO heeft de volgende rollen en verantwoordelijkheden:

- Adviseert en faciliteert de verwerkingsverantwoordelijken ten aanzien van het naleven en de uitvoering van het privacybeleid;
- Adviseert de verwerkingsverantwoordelijke bij datalekken (volgens de meldprocedure);
- Beheert het centrale verwerkingenregister;
- Opstellen van modellen, formats en standaard-overeenkomsten, waaronder o.a. de verwerkers-overeenkomst en de overeenkomst voor uitwisseling van persoonsgegevens;
- Draagt zorg voor het (laten) registreren van verwerkingen in het verwerkingsregister;
- Adviseert de verwerkingsverantwoordelijke bij het uitvoeren van DPIA's en de daaruit voortvloeiende risico's. Ook over maatregelen om deze tegen gaan;
- Adviseert over de bepalingen in verwerkersovereenkomsten en faciliteert bij het opstellen, aanpassen en uitonderhandelen daarvan;
- Adviseert over de verwerkingsgrondslag;
- Adviseert samen met de CISO over bewustmakingsprogramma's- en privacytrainingen voor medewerkers;
- Adviseert de verwerkingsverantwoordelijke over Privacy by Design & Default bij ontwikkeling van nieuwe systemen in samenwerking met de CISO;
- Ondersteunt en faciliteert verwerkingsverantwoordelijke bij het afhandelen van datalekken volgens de meldprocedure.

#### **Andere rollen en verantwoordelijkheden**

| Afdeling / Functionaris | Betrokkenheid                                                                                                                                                                                                                                                                                                         |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Gemeentejurist          | Ondersteunen van Privacy Officer ten aanzien van privacyvraagstukken en adviseren over privacy gerelateerde bepalingen in overeenkomsten.                                                                                                                                                                             |
| CISO                    | Toepassing en implementatie van technische en organisatorische maatregelen voor de bescherming van persoonsgegevens. Tijdig melden van Informatiebeveiligingsincidenten bij Privacy Officer en de Functionaris Gegevensbescherming als er mogelijk sprake is van betrokkenheid van persoonsgegevens bij het incident. |
| Communicatie            | Als communicatie (intern en extern) een rol speelt worden medewerkers van communicatie betrokken.                                                                                                                                                                                                                     |
| Audit / Concern Control | Toetst het goed en betrouwbaar functioneren van de gehele interne organisatie.                                                                                                                                                                                                                                        |
| Informatiemanagement    | Inrichten van de informatievoorziening (de beoordeling van welke functionaliteit en welke data in op welke wijze / in welk systeem verwerkt kan / moet worden).                                                                                                                                                       |

#### Overlegstructuren

1. De burgemeester als portefeuillehouder bespreekt periodiek met de Functionaris Gegevensbescherming.
2. De burgemeester, de gemeentesecretaris en de Functionaris Gegevensbescherming bespreken jaarlijks de voortgang aan de hand van het jaarverslag van de Functionaris Gegevensbescherming.
3. Het Managementteam bespreekt drie keer per jaar met de Functionaris Gegevensbescherming, de Chief Information Security Officer en de Privacy Officer de voortgang aan de hand van het jaarlijkse uitvoeringsprogramma informatiebeveiliging en privacy. Actuele onderwerpen en het jaarverslag van de Functionaris Gegevensbescherming komen ook aan de orde.
4. Er is een werkgroep Informatiebeveiliging en privacy. Naast de Functionaris Gegevensbescherming, de Chief Information Security Officer en de Privacy Officer zitten in deze werkgroep medewerkers van alle afdelingen.
5. De Concerncontroller, de Functionaris Gegevensbescherming en de Chief Information Security Officer hebben periodiek overleg over informatiebeveiliging en privacy.
6. Er is een aanjaagteam dat bestaat uit de Functionaris Gegevensbescherming, de Chief Information Security Officer en de Privacy Officer. Zij overleggen maandelijks over informatiebeveiliging en privacy.

*Vastgesteld op 11 november 2025 door burgemeester en wethouders van Goes.*