gemeente Tholen

GEMEENTEBLAD

Officiële uitgave van de gemeente Tholen

Nr. 58073

10 februari

2026

Privacyreglement Tholen 2025 - 2027

Het college van burgemeester en wethouders van Tholen,

gelezen het voorstel d.d. 11-12-2025

overwegende dat:

het normenkader NOREA voorschrijft dat een privacyreglement binnen 3 jaar moet worden herzien

gelet op AVG art. 4, art. 24 en art. 32(5)

besluit:

1. het privacyreglement Tholen 2025 - 2027 vast te stellen
2. te bepalen dat dit beleid in werking op de dag na die van bekendmaking
3. te bepalen dat privacyreglement 2022 – 2025 komt te vervallen door de vaststelling

Privacyreglement Tholen 2025

In dit reglement laat gemeente Tholen zien op welke manier zij dagelijks omgaat met persoonsgegevens en privacy, en wat er wettelijk wel en niet verantwoord is. Het betreft een uitgebreide uiteenzetting van het privacybeleid.

Privacy speelt een belangrijke rol in de relatie tussen de burger, ondernemers en de overheid en staat daarmee hoog op de bestuurlijke agenda. Gemeenten hebben de verantwoordelijkheid over persoonsgegevens en gegevensuitwisseling op alle terreinen waar ze actief zijn. Gemeenten zijn verplicht om zorgvuldig en veilig, proportioneel en vertrouwelijk om te gaan met het verzamelen, bewaren en beheren van persoonsgegevens van burgers. Dat geldt voor alle taken van de gemeente, waaronder taken op het gebied van basisadministraties, openbare orde en veiligheid, en het sociaal domein.

1. Wetgeving en definities

Sinds 25 mei 2018 is de Algemene Verordening, hierna afgekort tot AVG, van toepassing in alle lidstaten van de Europese Unie. De AVG heeft als doel om het recht op bescherming van persoonsgegevens te waarborgen in alle lidstaten van de Europese Unie.

De gemeente Tholen hanteert de definities zoals beschreven in artikel 4 van de AVG.

Buiten de AVG zijn er ook andere, vakspecifieke, wetgeving die zorgen voor een bescherming van persoonsgegevens:

- De Uitvoeringswet AVG;
- De Wet Open Overheid (WOO);
- De wet Basisregistratie Personen (wet BRP);
- De Wet Politiegegevens (Wpg);
- De Participatiewet;
- De Jeugdwet.

2. Reikwijdte

Het reglement is van toepassing op alle verwerkingen van persoonsgegevens (zowel inwoners, ondernemers als medewerkers) door alle bestuursorganen van de gemeente (commissies, burgemeester, college van burgemeester en wethouders en gemeenteraad). Oftewel: voor alle verwerkingen die binnen de gemeentelijke organisatie plaatsvinden.

3. Verantwoordelijke

De bestuursorganen van de gemeente zijn onder andere de onafhankelijke commissies, burgemeester, het college van burgemeesters en wethouders (college van B&W) en de Raad. Gemeentelijke onderdelen is verantwoordelijk voor een deel van de gegevensverwerkingen binnen de gemeentelijke organisatie.

In het register van verwerkingen staat per proces, waar persoonsgegevens verwerkt worden, aangegeven welk orgaan de verwerkingsverantwoordelijke is.

4. Verwerkingen (Artikel 4, AVG)

De verwerking van persoonsgegevens is elke handeling of elk geheel van handelingen met persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde processen. In de AVG valt onder een verwerking:
- Verzamelen, vastleggen en ordenen;
- Bewaren, bijwerken en wijzigen;
- Opvragen, raadplegen, gebruiken;
- Verstrekken door middel van doorzending;
- Verspreiding of enige andere vorm van ter beschikkingstellen;
- Samenbrengen, met elkaar in verband brengen;
- Afschermen, uitwissen of vernietigen van gegevens.

Uit deze opsomming blijkt dat alles wat je met een persoonsgegeven doet een verwerking is.

4.1. Doeleinden (Artikel 5, AVG)
Volgens de wet mogen persoonsgegevens alleen verzameld worden als daarvoor een doel is vastgesteld. Het doel moet uitdrukkelijk omschreven en gerechtvaardigd zijn. De gegevens mogen niet voor andere doelen verwerkt worden. Voor de uitvoering van sommige wetten, zoals bijvoorbeeld de Jeugdwet, zijn de doelen voor het verwerken in de wet al vastgelegd, net als de persoonsgegevens die gevraagd en verwerkt mogen worden. Gemeente Tholen legt de doelen van gegevensverwerkingen vast in het register van verwerkingen.

4.2. Rechtmatige grondslag (Artikel 6, AVG)
Voor elke verwerking van persoonsgegevens moet een rechtmatige grondslag uit de wet van toepassing zijn. Dat betekent dat de verwerking alleen mag plaatsvinden:
- Om een verplichting na te komen die in de wet staat;
- Voor de uitvoering van een overeenkomst waar de betrokkene partij is;
- Om vitale belangen te beschermen;
- Voor de goede vervulling van de gemeentelijke taak;
- Wanneer de betrokkene toestemming heeft gegeven voor de specifieke verwerking;
- Wanneer sprake is van een gerechtvaardigd belang.

De gemeente Tholen legt in het register van verwerkingen per proces, waar persoonsgegevens worden verwerkt, vast met welke rechtmatige grondslag deze verwerking plaatsvindt.

4.3. Wijze van verwerking
De hoofdregel van de verwerking van persoonsgegevens is dat het alleen toegestaan is in overeenstemming met de wet, en op een zorgvuldige wijze. Persoonsgegevens worden zoveel mogelijk verzameld bij de betrokkene zelf.

De wet gaat uit van subsidiariteit. Dit betekent dat verwerking alleen is toegestaan wanneer het doel niet op een andere, minder privacy-ingrijpende, manier kan worden bereikt. In de wet wordt ook gesproken over proportionaliteit. Dit betekent dat persoonsgegevens alleen mogen worden verwerkt als dit in verhouding staat tot het doel. Wanneer met geen, of minder (belastende), persoonsgegevens hetzelfde doel bereikt kan worden moet daar altijd voor gekozen worden.

De gemeente zorgt ervoor dat de persoonsgegevens kloppen en volledig zijn voordat ze verwerkt worden. Personen die deze gegevens verwerken zijn gebonden aan een geheimhoudingsplicht.

Daarnaast beveiligt de gemeente alle persoonsgegevens. Dit moet voorkomen dat de persoonsgegevens kunnen worden ingezien of gewijzigd door iemand die daar geen recht toe heeft. Hoe de gemeente dit doet staat in het informatiebeveiligingsbeleid van de gemeente en in een eventueel aanvullend beveiligingsplan specifiek opgesteld voor een proces of registratie.

4.4. Doorgifte (Artikel 44 t/m 50, AVG)
De gemeente geeft alleen persoonsgegevens door aan een land buiten de Europese Economische Ruimte (EER) of een internationale organisatie op grond van goedgekeurde afspraken door de Europese Commissie.

5. Verwerkingen (Wpg)

Gemeente Tholen heeft buitengewoon opsporingsambtenaren (BOA's) in dienst. De gegevens die BOA's gebruiken voor het opsporen van strafbare feiten en handhaven van de openbare orde worden politiegegevens genoemd.

De AVG geldt niet voor politiegegevens, maar betrokkenen waarvan politiegegevens worden verwerkt hebben ook recht op privacy. De regels daaromtrent zijn vastgelegd in de Wpg. De rechten van betrokkenen en verplichtingen voor gemeenten wijken wel af van de AVG, daarom wordt daaraan in dit beleid extra aandacht besteed.

De persoonsgegevens die gemeente Tholen verwerkt hebben tot doel om strafbare feiten op te sporen en daarop te handhaven. Enkele voorbeelden van persoonsgegevens die in dit kader verwerkt kunnen worden zijn:
- Identificerende gegevens, zoals naam, adres, woonplaats;
- Camerabeelden;
- Gegevens over strafbare gedragingen.

Er zijn verscheidene verplichtingen vanuit de Wpg waaraan de gemeente invulling geeft. Zo worden ook de verwerkingen van politiegegevens opgenomen in het verwerkingsregister. Daarnaast worden de politiegegevens in een separate, streng beveiligde applicatie verwerkt. De gemeente ziet toe op het autorisatiebeheer en logging van acties in deze applicatie. Verder zijn specifieke bewaartermijnen (in beginsel 5 jaar, met mogelijkheid tot verlengen) op grond van de Wpg ingericht. Over deze beveiligingsmaatregelen en omliggende processen worden periodiek interne en externe audits uitgevoerd.

Betrokkenen hebben vanuit de Wpg de volgende rechten:
- Recht op inzage.
- Recht op rectificatie.
- Recht op vernietiging.

Voor de uitvoering van deze rechten gelden in principe dezelfde procedures als voor de AVG.

Gegevens die onder de Wpg worden verwerkt, kunnen worden gedeeld met derden binnen het politiedomein (ter beschikking stellen) of daarbuiten (verstrekken). Verstrekking met betrekking tot de Wpg gebeuren op basis van de Verstrekkingenwijzer[1] van het BOA Registratiesysteem (BRS). Verdere verplichtingen en uitwerkingen van processen zijn opgenomen in het 'Handboek Wpg voor BOA's' van gemeente Tholen'.

6. Transparantie en communicatie

6.1. Wet Open Overheid (WOO)

Sinds 1 mei 2022 is de Wet Open Overheid (WOO) van toepassing. De WOO regelt het recht op informatie over alles wat de gemeente doet. Door middel van de WOO kan er informatie worden opgevraagd. Wanneer er informatie wordt opgevraagd kijkt de gemeente altijd of het antwoord geen inbreuk maakt op de persoonlijke levenssfeer van betrokkenen. In principe worden geen persoonsgegevens verstrekt.

6.2. Wet hergebruik van overheidsinformatie (who)

De Wet hergebruik van overheidsinformatie regelt het op verzoek verstrekken van overheidsinformatie voor hergebruik. Bij het verzoek bekijkt de gemeente altijd of het antwoord geen inbreuk maakt op de persoonlijke levenssfeer van betrokkenen. In principe worden geen persoonsgegevens verstrekt.

6.3. Informatieplicht (Artikel 13 en 14 AVG)

De gemeente informeert betrokkenen over het verwerken van persoonsgegevens. Wanneer betrokkenen gegevens aan de gemeente verstrekt, worden zij op de hoogte gesteld van de manier waarop de gemeente met persoonsgegevens om zal gaan. Dit is te vinden op de website van de gemeente in het 'Openbaar register van verwerkingen'. Daarnaast is hier het privacybeleid van de gemeente gepubliceerd.

6.4. Verwijdering

De gemeente bewaart persoonsgegevens niet langer dan nodig is voor de uitvoering van gemeentelijke taken, of zoals vastgelegd in de Archiefwet. Wanneer er nog persoonsgegevens opgeslagen zijn die niet langer nodig zijn voor het bereiken van het doel worden deze zo snel mogelijk verwijderd. Dit houdt in dat deze gegevens verwijderd worden, of zodanig worden aangepast dat de informatie niet meer gebruikt kan worden om iemand te identificeren.

1) https://www.natuurnetwerk.info/BRSdocumenten/Verstrekkingenwijzer.pdf

6.5. Rechten van betrokkenen (Artikel 13 t/m 20, AVG)
De wet bepaalt niet alleen de plichten van degenen die de persoonsgegevens verwerken, maar bepaalt ook de rechten van de personen van wie de gegevens worden verwerkt. Deze rechten worden ook wel de rechten van betrokkenen genoemd, en bestaan uit de volgende rechten:

- Recht op informatie: Betrokkenen hebben het recht om aan de gemeente te vragen of zijn/haar persoonsgegevens worden verwerkt;
- Inzagerecht: Betrokkenen hebben de mogelijkheid om te controleren of, en op welke manier, zijn/haar gegevens worden verwerkt;
- Correctierecht: Als duidelijk wordt dat de gegevens niet kloppen, kan de betrokkene een verzoek indienen bij de gemeente om dit te corrigeren;
- Recht van verzet: Betrokkenen hebben het recht aan de gemeente te vragen om hun persoonsgegevens niet meer te gebruiken;
- Recht om vergeten te worden: In gevallen waar de betrokkene toestemming heeft gegeven om gegevens te verwerken, heeft de betrokkene het recht om de persoonsgegevens te laten verwijderen voor zover een andere wettelijke verplichting dit niet onmogelijk maakt;
- Recht op bezwaar: Betrokkenen hebben het recht om bezwaar aan te maken tegen de verwerking van zijn/haar persoonsgegevens. De gemeente zal hieraan voldoen, tenzij er gerechtvaardigde gronden zijn voor de verwerking.

Om gebruik te maken van zijn/haar rechten kan de betrokkene een verzoek indienen. Dit verzoek kan via de website met behulp van DigiD worden ingediend. Daarnaast kan er via een afspraak op het gemeentehuis een verzoek ingediend worden met het formulier dat op de website staat.

De gemeente heeft vier weken de tijd, vanaf de ontvangst van het verzoek, om te beoordelen of het verzoek gerechtvaardigd is. Binnen vier weken zal de gemeente laten weten wat er met het verzoek gaat gebeuren. Als het verzoek niet wordt opgevolgd is er de mogelijkheid om bezwaar te maken bij de gemeente, of een klacht in te dienen bij de Autoriteit Persoonsgegevens (AP). Naar aanleiding van een verzoek kan de gemeente aanvullende informatie opvragen om zeker te zijn van de identiteit van de betrokkene.

7. Inzet van camera's

Binnen de gemeente wordt onder bepaalde omstandigheden gebruik gemaakt van cameratoezicht, zoals vastgelegd in de Gemeentewet. Camera's kunnen een grote inbreuk maken op de privacy van diegene die gefilmd worden. Om de privacy zo goed mogelijk te waarborgen worden er eisen gesteld aan de inzet van camera's. Voor de inzet van camera's heeft de gemeente Tholen een intern camera-protocol opgesteld.

8. Cookies

Een cookie is een klein tekstbestand dat bij het eerste bezoek aan de website van de gemeente wordt opgeslagen. Websites moeten bezoekers toestemming vragen voor plaatsing van cookies. De cookiewet maakt een uitzondering voor cookies die niet privacygevoelig zijn. Bijvoorbeeld voor cookies die bezoekersaantallen bijhouden. Gemeente Tholen gebruikt alleen technische en functionele cookies. De cookies die wij gebruiken zijn noodzakelijk voor de technische werking van de website.

9. Plichten van de gemeente

De gemeente heeft een aantal verplichtingen o.g.v. de AVG, de belangrijkste worden hieronder weergegeven.

9.1. Register van verwerkingen (Artikel 30, AVG)
De gemeente is verantwoordelijk voor het aanleggen en onderhouden van een register van alle verwerkingen waarvan de gemeente de verwerkingsverantwoordelijke is. Elke verwerking bevat een beschrijving van wat er tijdens een verwerking plaatsvindt, en welke gegevens daarvoor worden gebruikt, namelijk:

- De naam en contactgegevens van de verwerkingsverantwoordelijke en, mogelijk, de gezamenlijke verwerkingsverantwoordelijke;
- De doelen van de verwerking;
- Een beschrijving van het soort persoonsgegevens en de daarbij horende betrokkenen;
- Een beschrijving van de ontvangers van de persoonsgegevens;
- Een beschrijving van het delen van persoonsgegevens aan een derde land of internationale organisatie;
- De termijnen waarin de verschillende persoonsgegevens moeten worden gewist;
- Een algemene beschrijving van de beveiligingsmaatregelen.

9.2. Gegevensbeschermingseffectbeoordeling (Artikel 35, AVG)
Met een gegevensbeschermingseffectbeoordeling worden de effecten en risico's van nieuwe of bestaande verwerkingen beoordeeld op de bescherming van de privacy. De gemeente voert deze uit wanneer er een geautomatiseerde verwerking, een grootschalige verwerking, of wanneer er een grootschalige monitoring van openbare ruimten plaatsvindt. Dit geldt in het bijzonder bij verwerkingen waarbij nieuwe technologieën worden gebruikt.

Het uitvoeren van een DPIA is niet altijd verplicht. In geval van hogere risico's (bijvoorbeeld bij de verwerking van bijzondere persoonsgegevens, grootschalige verwerkingen, verwerkingen van bijzondere kwetsbare doelgroepen zoals jongeren, etc.) is een DPIA verplicht. Per DPIA wordt advies aan de FG gevraagd. Als uit een DPIA blijkt dat er sprake is van risicovolle verwerkingen zonder dat het mogelijk is hier maatregelen tegen te nemen wordt de Autoriteit Persoonsgegevens op de hoogte gesteld. De Autoriteit Persoonsgegevens maakt het overzicht met risicovolle verwerkingen openbaar.

De Privacy Officer heeft een uitvoerende functie bij het opstellen van een DPIA maar de proceseigenaren zijn verantwoordelijk voor het opstellen van de DPIA.

De gemeente heeft een procedure opgesteld voor de DPIA's.

9.3. Verwerkersovereenkomsten
Wanneer de gemeente externe partijen in de hand neemt om persoonsgegevens te verwerken wordt er een overeenkomst opgesteld tussen beide partijen voor de bescherming van persoonsgegevens. Deze overeenkomsten heten verwerkersovereenkomsten. In de overeenkomst worden afspraken gemaakt over:
- De doeleinden waarvoor de gegevens mogen worden verwerkt;
- Hoe de verwerker met de persoonsgegevens moet omgaan;
- Welke beveiligingsmaatregelen moeten worden genomen;
- Welke vormen van toezicht de eigenaar van de gegevens mag uitoefenen;
- De geheimhoudingsplicht;
- Inschakeling van derden en onderaannemers;
- Locatie van de data;
- Aansprakelijkheid in geval van schade door het niet naleven van regelgeving;
- Het vernietigen van persoonsgegevens na beëindiging van de overeenkomst.

9.4. Privacy by design/ Privacy by default
Privacy by Design houdt in dat vanaf het ontwerpen van een nieuw of aangepast proces, product, dienst of informatiesysteem wordt nagedacht over het rechtmatig, behoorlijk en transparant verwerken van persoonsgegevens en de maatregelen die hiervoor nodig zijn. Privacy by Default betekent dat de standaardinstellingen in systemen zijn ingesteld om maximale privacybescherming te borgen. De AVG noemt dit 'Gegevensbescherming door ontwerp en standaardinstellingen'. Bij het toepassen van Privacy by Design/Default wordt advies aan de FG gevraagd. De Privacy Officer kan ondersteunen bij het toepassen. De gemeente heeft een procedure opgesteld in het kader van Privacy by design/ privacy by default

9.5. Aanstellen van een Functionaris voor gegevensbescherming (FG) (Artikel 37 t/m 39, AVG)
De gemeente heeft een FG aangesteld. De FG is betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens. De taken van de functionaris zijn informeren, adviseren, toezicht houden, bewustwording creëren, en optreden als contactpersoon van de AP. Het is niet de bedoeling dat de functionaris de taken op het gebied van bescherming van de privacy van de afdelingen overneemt. De afdelingen hebben hun eigen verantwoordelijkheid in het goed omgaan met privacygevoelige gegevens. Een verwerking van persoonsgegevens wordt eerst aan de FG gemeld voordat de verwerking begint. De FG is verantwoordelijk voor het structureel toetsen van de implementatie en de uitvoering van de wettelijke eisen en de gemeentelijke richtlijnen op het gebied van privacy.
Voor vragen over privacy kunt u contact opnemen met de functionaris voor gegevensbescherming van gemeente Tholen via functionaris.gegevensbescherming@tholen.nl.

9.6. Datalekken (Artikel 33,34, AVG)
We spreken van een datalek wanneer persoonsgegevens in handen vallen van derden die geen toegang tot die gegevens mogen hebben, onbedoeld gewijzigd worden of onbedoeld niet langer beschikbaar zijn. Wanneer er een datalek heeft plaatsgevonden, die een risico kunnen vormen voor de vrijheden van betrokkenen meldt de gemeente dit zonder onredelijke vertraging, uiterlijk 72 uur nadat er kennis van de inbreuk is vernomen, aan de AP. Als dit later dan 72 uur is wordt er een motivering voor de vertraging bij de melding gevoegd. Het kan zijn dat de inbreuk een hoog risico met zich meebrengt voor de rechten en vrijheden van de betrokkenen. In dit geval meldt de gemeente dit aan de betrokkenen in eenvoudige en duidelijke taal. Om toekomstige datalekken te voorkomen worden bestaande datalekken

geëvalueerd. Niet alle datalekken hoeven te worden gemeld aan de AP en/of de betrokkene. Datalekken worden intern gemeld en onderzocht door de Privacy Officer.
De gemeente Tholen heeft voor haar medewerkers een werkinstructie opgesteld voor het melden van datalekken. In deze instructie staat ook aangegeven wanneer een datalek gemeld moet worden.

10. Rollen, taken en verantwoordelijkheden

In dit hoofdstuk zal er verder worden ingegaan op de rollen, taken en verantwoordelijkheden die horen bij het onderwerp privacy binnen de gemeente Tholen. De organisatie is in het kader van privacy ingedeeld in drie domeinen:
- College van B&W;
- Directie;
- De organisatie.

10.1. College van B&W
Het college van B&W van de gemeente Tholen is eindverantwoordelijk om te waarborgen dat persoonsgegevens worden beschermd in overeenstemming met wet- en regelgeving. Het college stelt ook kaders voor de bescherming van de privacy op basis van wet- en regelgeving.

10.2. Directie
De directie van de Gemeente Tholen:
- Is verantwoordelijk voor kaderstelling en sturing;
- Stuurt op gestelde kaders;
- Controleert of de getroffen maatregelen voldoende bescherming bieden om de privacy van betrokkenen te beschermen;
- Beoordeelt periodiek het privacybeleid op basis van de evaluatie en aanpassingen van het privacybeleid;
- Draagt er, op grond van artikel 38 lid 2 van de AVG, zorg voor dat de FG over voldoende middelen (waaronder tijd) ter beschikking wordt gesteld voor het vervullen van zijn taken en het in stand houden van zijn deskundigheid.

10.3. Organisatie

10.3.1. Teamleiders/proceseigenaren
De teamleiders/proceseigenaren zijn verantwoordelijk voor:
- Het uitvoeren van DPIA's voor verwerkingen met een hoog risico;
- Het zorgen voor de naleving van wet- en regelgeving;
- Zorgen voor de naleving van rechtmatige, behoorlijke en transparante verwerking van persoonsgegevens;
- Verantwoordelijk voor het zorgen voor bewustwording binnen de teams;
- Past privacy by design/ privacy by default toe;
- Verantwoordelijk voor de registratie van verwerkingsactiviteiten;
- Verantwoordelijk voor het melden van informatiebeveiligingsincidenten en datalekken binnen de organisatie;
- Verantwoordelijk voor het opstellen van verwerkersovereenkomsten;
- Zorgt dat de FG wordt betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens.

10.3.2. Functionaris Gegevensbescherming
De Functionaris Gegevensbescherming, FG, is binnen de organisatie een onafhankelijk toezichthouder op de toepassing van de AVG en Wpg en krijgt geen instructies over de uitvoering van taken. Ook krijgt de FG vanuit de directie voldoende middelen ter beschikking voor het vervullen van zijn taken. De FG mag naast zijn werkzaamheden eventueel andere functies vervullen maar er mag geen sprake zijn van belangenverstrengeling. De FG krijgt voorafgaand aan een verwerking van persoonsgegevens een melding van de proceseigenaar/manager.

De FG heeft minimaal de volgende taken:
- Informeert en adviseert de organisatie met betrekking tot het beschermen van persoonsgegevens;
- Toezien op de naleving van wet- en regelgeving en het vastgestelde beleid met betrekking tot bescherming van persoonsgegevens;
- Toezien op het toewijzen van verantwoordelijkheden, bewustmaking en opleiding van de organisatie op het gebied van de bescherming van persoonsgegevens;

- Adviseert voor welke verwerkingen een Data Protection Impact Assessment (DPIA) moet worden uitgevoerd en toetst de uitgevoerde DPIA's;
- Werkt samen met en treedt op als contactpersoon voor de Autoriteit Persoonsgegevens
- Evalueren van het privacybeleid (jaarlijks) en doet voorstellen tot implementatie en aanpassingen van het privacybeleid;
- Rapporteert rechtstreekst aan het college van B&W.

10.3.3. CISO

De Chief Information Security Officer, CISO, van de gemeente Tholen heeft ten aanzien van de privacybescherming een adviserende rol bij de DPIA's als het gaat om informatiebeveiliging. Ook adviseert de CISO bij informatiebeveiligingsincidenten in het kader van de meldplicht datalekken.

10.3.4. Privacy Officer

Naast de Functionaris voor de Gegevensbescherming is er een Privacy Officer aangesteld. Ten opzichte van de FG is de functie van de PO praktischer van aard. Hij/zij heeft een operationeel uitvoerende rol en is het dagelijkse aanspreekpunt voor medewerkers wat betreft gegevensbescherming. De Privacy Officer ondersteunt en adviseert de organisatie bij het opstellen van procedures, het afsluiten van verwerkersovereenkomsten, het vullen en bijhouden van het register van verwerkingen en het afhandelen van informatiebeveiligingsincidenten. De Privacy Officer heeft tevens een uitvoerende rol bij het opstellen van Data Protection Impact Assessments (DPIA's)

10.3.5. Alle medewerkers

Alle medewerkers (inclusief inhuur/externen) zijn verantwoordelijk voor de bescherming van de privacy van betrokkenen. Dat betekent dat iedereen zorgt voor een rechtmatige, behoorlijke en transparante verwerking van persoonsgegevens, gelet op de uitgangspunten subsidiariteit en proportionaliteit.

10.4 Matrix

Om de taken, rollen en verantwoordelijkheden op het gebied van de bescherming van persoonsgegevens inzichtelijk te maken is een RASCI-Matrix opgesteld. RASCI staat voor:

- Responsible (feitelijk verantwoordelijk)
- Accountable (eindverantwoordelijk)
- Supporting (uitvoerend)
- Consulted (adviserend, controlerend)
- Informed (geïnformeerd)

Tabel 2 Matrix

RASCI-model	Verantwoordelijkheid	Rol
Responsible	Feitelijk verantwoordelijk	– Directie – Teamleiders/proces-eigenaren – Alle medewerkers
Accountable	Eindverantwoordelijk	– College van B&W – Gemeenteraad – Burgemeester
Supporting	Ondersteunend	– Privacy Officer – CISO
Consulted	Adviserend	– CISO – FG
Informed	Geïnformeerd	– Gemeenteraad (in het kader van de Gemeentewet en de bestuurlijke toezichtstaak) – Inwoners – Alle medewerkers – Externe belanghebbenden

11. Afsluiting

Als de gemeente een wettelijke verplichting niet nakomt kan de betrokkene een klacht indienen. Deze zal via de klachtenregeling van de gemeente worden behandeld. In gevallen waar het reglement niets over zegt, beslist het verantwoordelijke bestuursorgaan van de gemeente. Ook heeft de betrokkene het recht om een klacht in te dienen bij de Autoriteit Persoonsgegevens. De betrokkene kan deze klacht indienen rechtstreeks bij de AP.

Tholen, 16 december 2025,

Burgemeester en wethouders van Tholen,

w.g. J.K. Fraanje
secretaris

w.g. M.L.P Sijbers
burgemeester