gemeente Tholen

GEMEENTEBLAD

Officiële uitgave van de gemeente Tholen

Nr. 81455

18 april

2018

Besluit van het college van burgemeester en wethouders van de gemeente Tholen houdende regels omtrent Privacy by design / privacy by default protocol

1 Inleiding

In het beleid van gemeente Tholen staat aangegeven welke principes wij hanteren om de persoonlijke levenssfeer van onze burgers te beschermen. Dit protocol is bedoeld om een aantal van die principes te kunnen honoreren.

Allereerst worden er in dit protocol definities gegeven. Vervolgens staat de doelstelling genoemd. Daarna volgt de paragraaf procedures, waarin aangegeven staat welke principes we hanteren en welke procedures we gebruiken.

2 Definities

Privacy by design: Het gaat erom dat de gegevensbescherming bij het ontwerp van de verwerking (proces, applicatie, enz.) als eis is meegenomen.
Privacy by default: De standaardinstellingen van de verwerking bieden een zo hoog mogelijk niveau van bescherming voor de betrokkene.
Functionaris gegevensbescherming: De gemeente heeft een functionaris gegevensbescherming (FG) aangesteld. Deze is verantwoordelijk voor de coördinatie en toetsing in dit proces.
Verantwoordelijke voor de applicatie: Het gaat hier om het afdelingshoofd van de afdeling die in het register van verwerkingen is aangeduid als interne verantwoordelijke voor de applicatie van de verwerking.

3 Doelstelling

De doelstelling van dit protocol luidt:
'Het leveren van een structuur en checklist voor het inregelen van privacy by design / privacy by default voor bestaande en nieuwe verwerkingen van persoonsgegevens.'

4 Procedures

Deze paragraaf behelst een lijst van principes die privacy by design / default bevorderen. Daarna worden procedures voor bestaande en nieuwe verwerkingen van persoonsgegevens benoemd.

4.1 Principes voor privacy by design /default

Iedere verwerking moet gecheckt worden op onderstaande principes [1] .

- **Minimaliseer**: Beperk zoveel mogelijk de verwerking van gegevens. Selecteer voor het verzamelen. Verwijder wanneer mogelijk.
- **Scheid**: Scheid persoonsgegevens zoveel mogelijk van elkaar en werk zo gedistribueerd mogelijk.
- **Abstraheer**: Aggregeer tot het hoogst mogelijke niveau. Beperk zoveel mogelijk het detail waarin persoonsgegevens worden verwerkt.
- **Bescherm**/maak onherleidbaar: Voorkom dat gegevens openbaar worden. Beveilig gegevens. Verbreek waar mogelijk de link tussen personen en gegevens (anonimiseer en pseudonimiseer).
- **Informeer**: Informeer gebruikers over de verwerking van hun persoonsgegevens.
- **Geef controle**: Geef gebruikers controle over de verwerking van hun persoonsgegevens.
- **Dwing af**: Stel een privacybeleid op en dwing dit af met technische en organisatorische middelen.
- **Toon aan**: Toon aan dat op een privacyvriendelijke wijze persoonsgegevens worden verwerkt. Verzamel logs, doe audits en rapporteer.

1) Rijksoverheid (2018). *Handreiking Algemene Verordening Gegevensbescherming.*

4.2 Bestaande verwerkingen

Gemeente Tholen verwerkt veel persoonsgegevens. Voor die verwerkingen bestaan uiteenlopende rechtsgrondslagen en doelen. Van de bestaande verwerkingen moeten de volgende zaken worden nagegaan. Daarvan moet tevens een registratie worden bijgehouden.

- De functionaris van gegevensbescherming (FG) houdt een register van verwerkingen bij.
- Per verwerking moet door de FG bepaald worden of deze aan de bovenstaande principes voldoen. De FG kan daarvoor medewerking verzoeken van de verantwoordelijke voor de verwerking.
- Vervolgens zijn er twee opties:
  - » De verwerking voldoet aan de principes. De verwerking wordt afgevinkt in een apart tabblad in het register van verwerkingen.
  - » De verwerking voldoet niet aan de principes:
    - Communicatie met de verantwoordelijke voor de verwerking door de FG
    - Plan opstellen hoe de principes kunnen worden gewaarborgd door FG en verantwoordelijke
    - Uitvoeren van het plan, verantwoordelijkheid ligt bij de verantwoordelijke, coördinatie bij de FG
    - Opnieuw toetsen van de verwerking op de principes door de FG
    - Registreren van de verwerking in het aparte tabblad in het register van verwerkingen door de FG

4.3 Nieuwe verwerking

Wanneer er een nieuwe verwerking van persoonsgegevens voorgenomen is moet deze ook voldoen aan de principes van privacy by design / default. Bij nieuwe verwerkingen kunnen twee situaties van toepassing zijn. Nieuwe verwerkingen van persoonsgegevens kunnen in bestaande applicaties worden gedaan. Daarnaast kunnen nieuwe verwerkingen in nieuwe applicaties worden gedaan. Bij nieuwe applicaties kan er een aanbestedingstraject gestart moeten worden. Vandaar dat er twee procedures zijn voor nieuwe verwerkingen.

4.4 Nieuwe verwerking in bestaande applicatie

Wanneer een nieuwe verwerking moet worden gedaan dient onderstaande werkwijze getoetst te worden.

- De verantwoordelijke voor de applicatie krijgt de aanvraag voor een nieuwe verwerking binnen
- De verantwoordelijke beoordeelt de verwerking
- Indien er persoonsgegevens worden verwerkt stelt de verantwoordelijke de FG op de hoogte van de verwerking wanneer de opdracht voor het ontwikkelen van de verwerking wordt doorgezet naar functioneel beheer en eventueel een LEAN expert wordt genotificeerd
- De FG toetst de opzet van de verwerking o.g.v. de rechtsgrondslag en aan de principes van privacy by design / default
- De FG overlegt met - en geeft advies aan de verantwoordelijke voor de verwerking, de aanvrager en functioneel beheer
- Eventueel wordt de verwerking aangepast
- De verwerking wordt opgenomen in het register van verwerkingen en het aparte tabblad voor de toetsing van de principes van privacy by design / default

4.5 Nieuwe verwerking in nieuwe applicatie

Bij de aankoop van nieuwe applicaties dienen we eisen te stellen aan de manier waarop met privacy wordt omgegaan. De nieuwe applicatie moet aan de principes van privacy by design / default voldoen. Dit is opgenomen in de Gemeentelijke Inkoopvoorwaarden Bij IT (GIBIT) voorwaarden.
Bij nieuwe verwerkingen in nieuwe applicaties wordt altijd het advies van de FG ingewonnen. Zijn toetsingskader voor de nieuwe applicatie omvat minstens de principes voor privacy by design / default.