Privacy by Design - open data van meldingen openbare ruimte

Bij het ontwerpen van de (open) data standaard is rekening gehouden met de gevolgen op het gebied van privacy. Het uitgangspunt is dat open data gepubliceerd dient te worden. In de standaard zijn geen persoonsgerelateerde velden opgenomen, zoals namen en contactgegevens. Wel kan in het open textveld of in toegevoegde bestanden privacygevoelige gegevens zitten. Daarom is gekeken of een DPIA verplicht is en welke andere privacywaarborgen kunnen worden ingebouwd.

**DPIA niet verplicht**

In de huidige opzet van het project is geen DPIA verplicht. De verwerking komt niet voor in de lijst met verwerkingen waarvoor een DPIA verplicht is[[1]](#footnote-1) en er is ook anderszin geen sprake van een zodanig hoog privacyrisico dat een DPIA zou moeten worden uitgevoerd. De uitgevraagde informatie betreft immers geen personen, maar objecten en situaties in de gemeente. Wel moeten er waarborgen worden ingebouwd om het project zo privacyvriendelijk mogelijk op te zetten (hierna). Bij wijzigingen in de verwerking, zoals wanneer meer velden worden toegevoegd, is het raadzaam om opnieuw te beoordelen of een DPIA nodig is.

**Toestemming vooraf en check achteraf voor risicovolle publicatie**

Bij het aanmaken van de melding dient de melder gevraagd te worden of het toegestaan is de data te publiceren. De melder moet op eenvoudige wijze worden geïnformeerd over *waarvoor* toestemming wordt gegeven. Indien aan dit criterium voldaan wordt en de privacy check is uitgevoerd (volgende kopje), mag de melding uitgebreid in de datapublicatie weer gegeven.

Let erop dat toestemming moet worden geregistreerd en de mogelijkheid moet worden geboden aan de betrokkene om zijn toestemming in te trekken. De melder moet op de hoogte worden gebracht van het feit dat hij zijn toestemming kan intrekken en hoe hij dat kan doen.

Indien openbaarmaking niet toegelaten is, dan mag de melding slechts beperkt gepubliceerd worden op enkel zaakniveau. Eventuele data die mogelijk (indirect) persoonsgegevens kunnen onthullen, zoals afbeeldingen, metadata van afbeeldingen waaronder gps gegevens, en onderdelen van tekstuele omschrijvingen die persoonsgegevens bevatten worden dan dus niet gepubliceerd.

**Privacy check**

Bij meldingen waarbij toestemming is gegeven voor publicatie is het nodig om een privacy check te doen, om te voorkomen dat melders – kwaadwillend of onbewust - zonder de juiste toestemming persoonsgegevens van andere personen delen. Er dient een correctie te worden uitgevoerd op de data door de behandelaar, danwel het dossier wordt op ‘geen toestemming’ gezet.

Indien de behandelaar niet zeker is of er sprake is van persoonsgegevens of dat deze mogen worden gepubliceerd kan hij terecht bij een privacyfunctionaris binnen de gemeente. Het is aan te raden om in de begin periode de behandelaars te laten samenwerken met een privacy functionaris om privacygevoeligheden in een melding te beoordelen. Nadat de behandelaar is ‘opgeleid’ op privacyvlak kan hij zelfstandig(er) beoordelingen maken. Daarnaast zijn andere waarborgen mogelijk, zoals periodieke bijeenkomsten van behandelaars om privacyissues in meldingen te bespreken of steekproefsgewijze controles door een privacyfunctionaris.

**Klachten over persoonsgegevens**

Indien een klacht over persoonsgegevens binnenkomt, dan kan de gemeente verantwoordelijk zijn om correcties uit te voeren. Een privacyfunctionaris dient de klacht in behandeling te nemen. Het is verplicht om bij de gemeente bekende hergebruikers (zoals apps, platformen) te informeren om ook correcties door te voeren. Of een datalekmelding nodig is bij de Autoriteit Persoonsgegevens staat ter beoordeling aan de privacyfunctionaris.

1. Zie <https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/stcrt-2019-64418.pdf>. [↑](#footnote-ref-1)