Handreiking toepassing privacy by design en privacy by default bij aanbestedingen

Auteur: Jasmijn de Pruis (Privacy Officer)
Datum: 21 november 2023
Versie: 1.0

Deze handreiking is tot stand gekomen op basis van de *Handleiding Privacy by Design* van het Centrum voor Informatiebeveiliging en Privacy (CIP) (versie 3.0).

Privacy by design en privacy by default
Gegevensbescherming door ontwerp en door standaardinstellingen, ofwel privacy by design en default is een verplichting vanuit de Algemene Verordening Gegevensbescherming (AVG). Deze principes bewerkstelligen een proactieve benadering van gegevensbescherming door het toepassen van privacycriteria en -maatregelen in vroeg stadium van het ontwerp en beheer van informatiesystemen en technologieën. Een informatiesysteem zal tenminste aan de volgende eisen moeten voldoen wanneer er sprake is van gegevensverwerking.

1. Dataminimalisatie
Voor iedere verzameling (en dus: verwerking) van persoonsgegevens geldt het vereiste dat deze toereikend, ter zake dienend en beperkt zijn tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt. Dit betekent dat alleen die persoonsgegevens mogen worden uitgevraagd die nodig zijn om het doel te bereiken, waarbij de verzamelde persoonsgegeven aantoonbaar in relatie staan tot het doel en dat het doel niet met minder gegevens kan worden bereikt. Onnodige uitvraging kan worden voorkomen door bij de analyse van de rechtmatigheid en noodzaak ook te kijken naar de voor de verwerking te verzamelen gegevens. Het informatiesysteem moet een functionaliteit bieden om invulling te geven aan dataminimalisatie.

2. Bewaren van gegevens
Persoonsgegevens mogen niet langer bewaard worden dan noodzakelijk. Wanneer het doel is bereikt en de gegevensverwerking niet meer noodzakelijk is zullen de gegevens bewaard moeten worden in een vorm die het mogelijk maakt de betrokkene niet langer te identificeren of worden vernietigd. Tevens zullen persoonsgegevens mogelijk vernietigd moeten worden indien de betrokkene een verzoek tot vernietiging van persoonsgegevens indient. Het informatiesysteem moet een functionaliteit bieden om bewaartermijnen te handhaven en persoonsgegevens vervolgens te vernietigen of te anonimiseren.

3. Toestemmingmanagement
Indien de gegevensverwerking is gebaseerd op de grondslag toestemming moet de betrokkene altijd de mogelijkheid krijgen om zijn of haar toestemming weer in te trekken. Toestemmingmanagement houdt in dat de betrokkene toestemming geeft om informatie te delen of in te zien. Het informatiesysteem moet een functionaliteit bieden om de toestemmingverlening en -intrekking bij te houden en daarnaast voor welke gegevensverwerkingen de betrokkene toestemming heeft verleend.

4. Transparantie bieden
Betrokkenen dienen geïnformeerd te worden over de gegevensverwerking. Daarnaast moeten zij worden gewezen op hun rechten. In de praktijk worden betrokkenen veelal geïnformeerd door middel van een privacyverklaring. Het informatiesysteem moet een mogelijkheid bieden tot het informeren van de betrokkenen.

5. Verlenen van inzage in persoonsgegevens

Betrokkenen hebben het recht op inzage in hun persoonsgegevens, dit betekent dat zij een overzicht kunnen opvragen van welke persoonsgegevens van hen worden verwerkt in een informatiesysteem. Het informatiesysteem moet een functionaliteit bieden om een dergelijk overzicht te kunnen genereren in een begrijpbaar en leesbaar formaat.

6. Rectificeren van persoonsgegevens

Betrokkenen hebben het recht om hun persoonsgegevens te laten rectificeren indien deze onjuist zijn. Het informatiesysteem moet een functionaliteit bieden zodat betrokkenen hun persoonsgegevens kunnen (laten) rectificeren.

7. Overdragen van persoonsgegevens

Betrokkenen hebben het recht om hun persoonsgegevens in een gestructureerde, gangbare en machineleesbare vorm te verkrijgen zodat zij deze indien nodig kunnen overdragen aan andere organisaties of instanties. Het informatiesysteem moet een functionaliteit bieden zodat betrokkenen hun persoonsgegevens kunnen (laten) overdragen.

8. Gegevensverwerking binnen de EER

Om een adequaat niveau van gegevensbescherming te kunnen handhaven is het noodzakelijk dat de verwerking van persoonsgegevens via het informatiesysteem plaatsvindt binnen de Europees Economische Ruimte (EER).