SPELREGELS VOOR DE DIGITALE STAD

1. De digitale infrastructuur moet bijdragen aan een leefbare, gezonde en veilige stad. De infrastructuur is er voor iedereen in de openbare ruimte van de stad, ongeacht sociale positie en inkomen. De infrastructuur is goed beschikbaar en toegankelijk en is toekomstvast en veilig. Zij is ingericht conform gemeentebrede standaarden en de Europese en landelijke wet- en regelgeving rond privacy en security.

2. De marktpartijen, instellingen, overheden en bewoners zijn producent en consument van de digitale infrastructuur en van de 'slimme diensten' die daar gebruik van maken. Samen, in co-creatie of alleen en waar dat voor hen wenselijk respectievelijk nodig is om het leven van burgers in de stad beter te maken en de stad te helpen zich economisch te ontplooien. De overheid regisseert en reguleert waar dat nodig is om de toegang, beschikbaarheid en de veiligheid van de digitale infrastructuur te waarborgen voor iedereen in de digitale stad.

3. De gebruikte technologie voor de digitale infrastructuur en Internet of Things is bekend, veilig (secure) en interoperabel, kent 'open interfaces', 'open protocollen' en maakt gebruik van 'open standaarden, tenzij…' landelijke of Europese standaarden anders aangeven. Deze zijn leidend. Bewoners weten welke apparatuur in 'hun omgeving' is geplaatst, hebben daar invloed op en kunnen daar gebruik van maken.

4. Data is 'open en gedeeld tenzij…' de wet- en regelgeving rondom privacy en security anders aangeeft en tenzij de data-eigenaar de data niet wil delen. De data over de bewoner is van de bewoner; zij is de eigenaar en beslist wat ermee gebeurt. De data van de digitale infrastructuur verzameld in en over de publieke ruimte is publiek goed.

OPEN DATA PRINCIPES

a. Data in de openbare ruimte (verder: “data”) zijn van eenieder. Deze data zijn publiek goed. Data die worden verzameld, gegenereerd of opgemeten (bijvoorbeeld door sensoren die in de openbare ruimte zijn geplaatst), moeten worden opengesteld, zodat iedereen daarvan gebruik kan maken voor commerciële en niet-commerciële doelen. Daarbij dient wel een privacy- en veiligheidsafweging te worden gemaakt.
b. Data kunnen persoonsgegevens bevatten. Deze data kunnen dus de levenssfeer van personen raken. De regels van de Wet bescherming persoonsgegevens zijn hierop van toepassing. Deze data moeten pas worden opengesteld nadat deze data zodanig zijn verwerkt (bijvoorbeeld geanonimiseerd of geaggregeerd) dat er geen privacy risico’s meer zijn.
c. Data die wel privacy of veiligheid risico’s meebrengen, mogen uitsluitend worden verwerkt binnen de kaders van de privacywetgeving. Opslag en verwerking van data dienen conform bestaande wetgeving uitgevoerd te worden.
d. Data die geen persoonsgegevens (meer) bevatten, dienen zodanig te worden geplaatst dat eenieder op een gelijkwaardige wijze toegang heeft tot die data (bijvoorbeeld via een Open Data portaal). Dat noemen we open stellen van data. Er worden geen technische of juridische belemmeringen opgeworpen die toegang tot data onmogelijk maken, beperken of discrimineren.
e. Data worden altijd kosteloos, zonder onnodige verwerkingen (waar mogelijk in de ruwe vorm) en volgens nader te bepalen functionele en technische eisen open gesteld.
f. Onderscheid wordt gemaakt met persoonlijke data (zoals een e-mail adres of betaalgegevens) welke met bewust medeweten en na een expliciete toestemming van personen worden verzameld. Gebruik van deze data wordt bepaald via een overeenkomst tussen betroffen partijen binnen de kaders van de privacywetgeving (zoals een gebruikersovereenkomst).
g. Gemeente heeft altijd inzicht in welke data in de openbare ruimte worden verzameld, onafhankelijk of de data wel of niet open gesteld kunnen zijn.
h. Gemeente blijft in dialoog met de partijen die bijdragen aan de data infrastructuur in de stad en streeft ernaar verdienmogelijkheden en een vruchtbaar economisch klimaat te creëren.