gemeente Krimpenerwaard

Gemeentelijk Cloudbeleid

Het gemeentelijke cloudbeleid is gebaseerd op de adviezen over de inkoop van cloudapplicaties van het Nationaal Cyber Security Centrum (NCSC) en de Informatiebeveiligingsdienst (IBD).

a) Dit beleid heeft vooral betrekking op diensten die worden afgenomen als software as a service (SAAS).
b) De GIBIT (meest recente versie) is van toepassing.
c) De leverancier committeert zich daarmee aan de VNG ICT-kwaliteitsnormen.
d) De gemeente moet vooraf nagedacht hebben over eventuele risico's van de clouddienst en de geïdentificeerde risico's moeten gemitigeerd zijn.
e) Het hoofdkantoor van de leverancier en het datacenter zijn gevestigd in de Europese Economische Ruimte. Buiten de EER moeten extra maatregelen genomen worden om aan de verplichtingen vanuit de Algemene Verordening Gegevensbescherming te voldoen. Ook moeten extra maatregelen genomen worden op basis van een risicoanalyse bij gebruik van een dienst van een dienstverlener die valt onder een juridisch regiem buiten dat van de AVG (ook al wordt de data in de EER opgeslagen). Er worden geen leveranciers of diensten gebruikt uit landen met een offensief cyberprogramma gericht tegen Nederlandse belangen.
f) Data blijven eigendom van de gemeente en moeten geanalyseerd kunnen worden met behulp van de business intelligence van de gemeente. Dit wordt opgenomen in de overeenkomst met de leverancier.
g) Er is een exit-strategie na afloop van het contract voor het overzetten van data naar een nieuwe applicatie. Dit wordt opgenomen in de overeenkomst met de leverancier.
h) Er is een dienstverleningsovereenkomst of servicelevel agreement waarmee afspraken over beheer, bereikbaarheid en continuïteit worden vastgelegd. Hierin wordt rekening gehouden met de servicenormen en openingstijden van de gemeente. In de dienstverleningsovereenkomst kunnen ook sanctiemogelijkheden staan bij het niet nakomen van de afspraken.
i) Technisch beheer berust bij de cloudleverancier, functioneel beheer berust bij de gemeente. Over het beheer worden vooraf afspraken gemaakt en vastgelegd. Een functioneel beheerder wordt aangewezen of aangesteld.
j) Cloudverbindingen verlopen via en worden gemonitord door de gemeentelijke servicebus. Koppelvlakken vinden plaats conform VNG en Common Ground standaarden.
k) Cloudverbindingen gaan bij voorkeur via het GGI-netwerk.
l) Applicaties koppelen ten behoeve van 2-factor authenticatie met de Active Directory.
m) Indien de applicatie persoonsgegevens verwerkt wordt er een verwerkersovereenkomst afgesloten conform VNG-model. Opgenomen zijn in ieder geval de karakteristieken van gebruik van een clouddienst, zoals de (hoofd-) dienstverlener en eventuele onder-dienstverleners, het type dienstverlening (public/private/hybride/community cloud), de geografische regio van verwerking en opslag van gegevens.
n) In de overeenkomst met de dienstverlener wordt opgenomen dat de dienstverlener controle en verantwoordingsonderzoeken toelaat of daarover rapporteert; er bestaat een 'right-to-audit' voor de opdrachtgevende organisatie.
o) De applicatie moet kunnen archiveren "by design". Dit betekent dat bij vernietiging van geproduceerde documenten het ook mogelijk moet zijn metadata en procesinformatie in de applicatie mee te vernietigen. Ook als documenten via een automatische koppeling worden gearchiveerd in een zaaksysteem.
p) De opdrachtnemer garandeert dat gedurende de contractperiode de aangeboden oplossing wordt onderhouden, ondersteund en doorontwikkeld.

q) Wijzigingen in de oplossing (beheer en doorontwikkeling) worden eerst door de opdrachtnemer uitvoerig getest en pas daarna in de productieomgeving doorgevoerd. Opdrachtgever wordt van te voren op de hoogte gesteld van wijzigingen (release notes).
r) Opdrachtnemer voorziet in een beveiligde SaaS omgeving en houdt deze veilig door het direct uitvoeren van beschikbare beveiligingspatches.
s) Onderdeel van de SaaS-oplossing is het adequaat beschikbaar hebben van een volledige en goed functionerende backup- en restore voorziening.