

Richtlijn globale aansluitvoorwaarden informatieveiligheid en privacy

Informatieveiligheid:

- Op alle (ICT-)inkopen van de gemeente De Ronde Venen zijn de GIBIT-inkoopvoorwaarden van toepassing. (<https://www.vngrealisatie.nl/gibit>). Specifiek de artikelen opgenomen onder “II Privacy, beveiliging en archivering”.
- De leverancier moet een actuele NEN/ISO-27001 certificering hebben. De ontwikkeling, beheer en onderhoud van de oplossing moeten binnen de scope van de certificering vallen. Alternatief hiervoor is de NEN-7510 certificering of de BIO (Baseline Informatieveiligheid Overheden). De certificeringen moeten geldig en actueel zijn. De laatste audit moet minder dan een jaar geleden hebben plaatsgevonden. Graag ontvangen we het certificaat en de bijbehorende scoop (verklaring van toepasselijkheid). In de overeenkomst moet ook het auditrecht worden opgenomen.
- De oplossing moet voldoen aan de internet- en beveiligingsstandaarden van het Forum Standaardisatie. Zie hiervoor <https://www.forumstandaardisatie.nl/open-standaarden/lijst/verplicht>
- De oplossing moet ontwikkeld zijn met privacy en informatieveiligheid by design.
- De data van gemeente De Ronde Venen moet binnen de grenzen van de EU (met uitzondering van Groot Brittannië) verwerkt en opgeslagen worden. Dit kan dus ook in één van de datacenters van de gemeente zelf zijn.
- Alle data van gemeente De Ronde Venen die buiten haar eigen datacenters bewaard wordt, moet encrypted zijn. Dit is tijdens transport, verwerking en opslag. De encryptie-sleutel moet apart van de data bewaard worden op een beveiligde plek.
- Netwerkverbindingen tussen de gemeente De Ronde Venen en de leverancier lopen bij voorkeur via het Diginetwerk.
- Er moet in de hoofdovereenkomst beschreven staan hoe er wordt omgegaan met data-sanering, backup/herstel, archivering.
- Er moet in de overeenkomst een exit-strategie beschreven staan. Alle data is en blijft van gemeente De Ronde Venen en moet na afloop van de overeenkomst in een gangbaar formaat aan de gemeente overhandigd worden. Ook moet de procedure van datavernietiging beschreven zijn.
- Het gebruik van basisregistraties is verplicht. Er moet een goede, werkende aansluiting beschreven worden op onze basisregistraties (API's). Bij gebruik van de BRP (Basisregistratie Personen) moet de oplossing vallen binnen het autorisatiebesluit.
- Voor authenticatie moet gebruik gemaakt worden van de Multi-Factor Authenticatie oplossing van de gemeente (2FA, Microsoft Authenticator) of de Single Sign On oplossing van de gemeente (Azure AD). Er moet in logging voorzien zijn.

Privacy:

- Er moet aantoonbaar voldaan worden aan de Algemene Verordening Gegevensbescherming (AVG). In aanvulling/aansluiting op Gibit en met verwijzing naar het door VNG gehanteerde normenkader (https://www.informatiebeveiligingsdienst.nl/wp-content/uploads/2019/10/VNG_AVG_borging_okt-2019.pdf) benoem ik specifiek.:
 - Er wordt voldaan aan geformuleerd, geaccordeerd en gepubliceerd privacybeleid en reglement.
 - Ten grondslag liggende werkprocessen zijn vastgesteld waarbij verwerkingsactiviteiten worden onderkend en opgenomen in het register van verwerkingsactiviteiten.
 - De verwerkingsactiviteiten zijn getoetst aan de beginselen van de AVG (artikel 5 en 6).
 - Er wordt voorzien in de facilitering van de rechten van betrokkenen alsmede functionaliteit voor de vastlegging en intrekking van toestemming als grondslag voor de verwerkingsactiviteit.
 - Daar waar noodzakelijk wordt volgens standaard procedure en format zo snel als mogelijk een DPIA uitgevoerd waarmee invulling gegeven kan worden aan het principe van PbyDesig/Default.
 - Proces- en/of Systeembeheerder (key-user) zijn aanspreekpunt voor de privacy organisatie en dragen zorg voor de borging van de privacy beginselen binnen het werkveld.
 - Er wordt voldaan aan het staande beleid op het gebied van autorisatie en logging.
 - De OR wordt betrokken wanneer het gaat om het verwerken van alsmede de bescherming van de persoonsgegevens van medewerkers.
- Aansluiting op VNG ontwikkelingen m.b.t. bijvoorbeeld een referentie verwerkingsregister is gewenst met duiding van onderhavige Gemmacomponent(en).
- Privacy by default van gemeente De Ronde Venen, zie Privacy Handboek, bijlage 4 (intranet of bij de Privacy Adviseur).