Instituut
Fysieke
Veiligheid

Veiligheidsregio ICT-kwaliteitsnormen

Behorende bij GIBIT 2016
(Gemeentelijke Inkoopvoorwaarden bij IT)

Versie: Definitief, januari 2020

Instituut Fysieke Veiligheid
Postbus 7010
6801 HA Arnhem
Kemperbergerweg 783, Arnhem
www.ifv.nl
info@ifv.nl
026 355 24 00

Colofon

Titel:	Veiligheidsregio ICT-kwaliteitsnormen
Datum:	1 januari 2020
Status:	Definitief
Versie:	januari 2020

1 Inleiding

In december 2016 zijn de Gemeentelijke Inkoopvoorwaarden bij IT(GIBIT) door de Vereniging van Nederlandse Gemeenten (VNG) vastgesteld. Het betreft een set uniforme en gestandaardiseerde inkoopvoorwaarden die gemeenten en gemeentelijke samenwerkingsverbanden kunnen gebruiken bij de inkoop van ICT Prestaties. De reikwijdte betreft alle producten en/of diensten die gemeenten en gemeentelijke samenwerkingsverbanden op het gebied van ICT verwerven (een nadere specificatie van deze reikwijdte is gegeven in de toelichting op de GIBIT).
Opdrachtgevers wensen een ICT Prestatie te gebruiken binnen hun Applicatielandschap. Hiervoor is het nodig dat de ICT Prestatie goed aansluit op dat applicatielandschap en dat de ICT Prestatie voldoet aan bepaalde normen, bijvoorbeeld op gebied van beveiliging. Deze normen zijn meer aan verandering onderhevig dan de GIBIT, vandaar dat incidenteel of sporadisch bijgewerkte normen en standaarden voor ICT-producten en diensten gepubliceerd worden.
De GIBIT is tevens geadopteerd door andere decentrale overheden zoals GGD'en, GHOR bureaus en Veiligheidsregio's. Op deze organisaties zijn andere sectorale referentiearchitecturen van toepassing met eigen specifieke normen en standaarden voor ICT-producten en diensten. Om die reden zijn bij die organisaties niet de Gemeentelijke ICT-Kwaliteitsnormen van toepassing, maar de ICT-Kwaliteitsnormen behorend bij de betreffende sector.
Dit document betreft de specificatie van de Veiligheidsregio ICT-kwaliteitsnormen die een onderdeel vormen van de GIBIT (in plaats van de Gemeentelijke ICT-kwaliteitsnormen). Ook wordt in dit document toegelicht op welke wijze de Veiligheidsregio ICT-kwaliteitsnormen onderhouden worden en gebruikt kunnen worden.
De Veiligheidsregio ICT-kwaliteitsnormen wordt gepubliceerd door het Instituut Fysieke Veiligheid (IFV) op softwarecatalogusvr.nl/inkoopondersteuning en wordt incidenteel voorzien van bijgewerkte normen en standaarden voor ICT-producten en diensten.

1.1 Reikwijdte Veiligheidsregio ICT-kwaliteitsnormen

De Veiligheidsregio ICT-kwaliteitsnormen betreffen normen en standaarden die verplicht zijn. De verplichting kan volgen uit:

1. Een wettelijk kader; en/of
2. Standaarden op de lijst van open standaarden (pas-toe-of-leg-uit); en/of
3. Standaarden die als landelijke veiligheidsregio standaard of norm zijn vastgesteld.

Elke norm die gehanteerd wordt, is vastgesteld. Standaarden of versies van standaarden die nog in ontwikkeling zijn vallen dan ook niet binnen de Veiligheidsregio ICT-kwaliteitsnormen. Pas zodra een nieuwe standaard vastgesteld wordt en de status "in gebruik" krijgt, wordt deze standaard toegevoegd aan de Veiligheidsregio ICT-kwaliteitsnormen.
Het vaststellingsproces kan per norm verschillen, dit is mede afhankelijk van de beheerder en governance structuur van de betreffende norm. Voor wettelijke normen valt dit onder verantwoordelijkheid van de wetgever. Landelijk vastgestelde open standaarden worden vastgesteld door het Nationaal Beraad Digitale Overheid en het Forum Standaardisatie. Specifiek Veiligheidsregio standaarden worden vastgesteld onder regie van de

Architectuurboard van de Veiligheidsregio's. Hiervoor is een standaardisatieproces ingericht waarbij Veiligheidsregio's nauw betrokken zijn en mede bepalen wat de norm / standaard wordt. In veel gevallen worden ook ICT leveranciers nauw betrokken.

De normen hebben betrekking op de volgende ICT kwaliteitsgebieden:

- architectuur
- interoperabiliteit
- informatiebeveiliging
- dataportabiliteit
- toegankelijkheid
- archivering
- generieke digitale infrastructuur (GDI) en de basisregistraties
- documentatie
- e-facturering

In dit document zijn voor elk bovengenoemd ICT-kwaliteitsgebied het doel, de reikwijdte en de standaarden/normen opgenomen welke binnen de GIBIT vallen.

1.2 Veiligheidsregio ICT-kwaliteitsnormen binnen overeenkomststructuur

De binnen de GIBIT voorgeschreven normen en standaarden zijn minimumeisen. Doordat in de GIBIT expliciet naar deze normen wordt verwezen, zijn deze geborgd in de Overeenkomst die gesloten wordt. In de beschrijving van de vereisten (bestek) die een Opdrachtgever maakt, kan de Opdrachtgever extra vereisten aangeven (bijvoorbeeld vereisen dat bepaalde aanbevolen standaarden ook verplicht moeten worden ondersteund). Zie onderstaand figuur voor een schematisch overzicht tussen de Overeenkomst, de onderliggende GIBIT met Veiligheidsregio ICT-kwaliteitsnormen en de vereisten die door Opdrachtgever gesteld kunnen worden.

1.3 Toepassing van de Veiligheidsregio ICT-kwaliteitsnormen

Door gebruik van de GIBIT worden de Gemeentelijke ICT-kwaliteitsnormen van toepassing verklaard (artikel 6.1). Dit is dus indien een Overeenkomst wordt gesloten waar de GIBIT van toepassing is verklaard, als in geval een Opdrachtgever bij een uitvraag (bijvoorbeeld bij een aanbesteding) aangeeft dat de GIBIT van toepassing is.
Voor Veiligheidsregio's zal in de aanbesteding aangegeven worden dat de Veiligheidsregio ICT-kwaliteitsnormen van toepassing zijn in plaats van de Gemeentelijke ICT-kwaliteitsnormen. De GIBIT zelf wordt/is niet aangepast en zal dus verwijzingen naar de Gemeentelijke ICT-kwaliteitsnormen blijven houden (zoals ook in het vervolg van deze paragraaf waar aan de GIBIT gerefereerd wordt). In de laatste alinea volgt nog de aanvulling hoe om te gaan met nieuwe versies van de Veiligheidsregio ICT-kwaliteitsnormen.

In artikel 6.1 wordt onder meer het volgende bepaald:

- 6.1: Het Overeengekomen gebruik omvat dat de ICT Prestatie ("de te leveren goederen en diensten") voldoet aan de Gemeentelijke ICT-kwaliteitsnormen. Mede gezien de definitie van Overeengekomen gebruik (artikel 1.23) volgt hier dus uit dat Leverancier geacht is bekend te zijn met de Gemeentelijke ICT-kwaliteitsnormen, immers, die zijn deel van de GIBIT en het betreft documenten die vooraf bekend zijn;
- 6.1 i: Deze bepaling limiteert welke Gemeentelijke ICT-kwaliteitsnormen gelden. Enerzijds door de tijdsbepaling dat die versie van de Gemeentelijke ICT-kwaliteitsnormen geldt die ten tijde van het sluiten van de Overeenkomst voorligt. Anderzijds door de toespitsing op de voor de functie en het werkingsgebied relevante Gemeentelijke ICT-kwaliteitsnormen;
- 6.1 ii: Los van de vastgestelde Gemeentelijke ICT-kwaliteitsnormen staat het Opdrachtgever vrij om extra normen voor de specifieke opdracht te stellen. Deze dienen dan door de Opdrachtgever extra gespecificeerd te zijn in de aanbestedingsstukken.

Artikel 6.2 t/m 6.5 betreft artikelen die toezien op het uitvoeren van (preventieve) testen van de ICT Prestatie ten aanzien van de geldende Gemeentelijke ICT-kwaliteitsnormen. Bij de Gemeentelijke ICT-kwaliteitsnormen wordt per norm aangegeven welke testvoorzieningen daarvoor beschikbaar zijn en gebruikt dienen te worden.
Artikel 6.4 bepaalt dat bij de Acceptatieprocedure getoetst wordt of voldaan is aan de normen die gesteld zijn in artikel 6.1.
Zoals toegelicht betreft artikel 6 de eisen ten tijde van het komen tot een Overeenkomst en de Acceptatie. In artikel 8.9 sub iii is een bepaling opgenomen omtrent het bijblijven met nieuwe versies van de Gemeentelijke ICT-kwaliteitsnormen ten tijde van de duur van de Overeenkomst. Hiermee wordt geborgd dat de ICT Prestatie blijvend voldoet aan de actuele normen. Overigens, conform artikel 8.1 kunnen afspraken gemaakt worden over vergoedingen voor deze verplichting. Aangezien de Gemeentelijke ICT-kwaliteitsnormen alle officieel vastgestelde normen zijn, is vaak vroegtijdig bekend welke normen toegevoegd dan wel aangepast worden. Bij vaststelling van (aangepaste) normen is meestal sprake van een overgangsperiode. Bij wetgeving is dit meestal de periode tussen vaststelling en het daadwerkelijk ingaan van een wet. Bij de door VNG/VNG Realisatie vastgestelde normen en standaarden wordt veelal via een addendum op het VNG Realisatie convenant een specifieke afspraak gemaakt met betreffende leveranciers over onder meer de

overgangsperiode. De verplichting om te blijven voldoen aan de Gemeentelijke ICT-kwaliteitsnormen is verder verwoord in artikel 10.1 sub v alwaar dit als garantie is verwoord.

Voor de Veiligheidsregio ICT-kwaliteitsnormen is een gelijke afspraak van kracht analoog aan het bovenstaande. De Architectuurboard van de Veiligheidsregio's stellen de normen en standaarden vast en nemen deze op in nieuwe versies van de Veiligheidsregio ICT-kwaliteitsnormen. Wanneer een overgangsperiode van toepassing is dan wordt dat vermeld hierbij. In tegenstelling tot VNG Realisatie sluit het IFV en de Architectuurboard geen convenanten met leveranciers. Leveranciers gaan bij het aangaan van een Overeenkomst hiermee impliciet akkoord met overgangsperiodes voor het conformeren aan nieuwe normen en standaarden.

2 Architectuur

2.1 Doel

Veiligheidsregio's hebben een breed taken- en dienstenpakket. Gevolg is dat er een landschap van verschillende informatiesystemen nodig is om goed invulling te kunnen geven aan die taken en diensten. Er is behoefte aan inzicht en overzicht ten aanzien van dat landschap om goed te kunnen sturen en organiseren.

2.2 Reikwijdte

Voor de ICT Prestatie geldt de Veiligheidsregio Referentie Architectuur (VeRA) als kader. Deze sectorale referentiearchitectuur beschrijft de inrichting van de gewenste informatiehuishouding van Veiligheidsregio's en de aansluiting daarvan op de omgeving. De informatiehuishouding bestaat onder meer uit referentiecomponenten en applicatie-functionaliteit waarmee de gegevens kunnen worden opgeslagen, geraadpleegd en processen kunnen worden ondersteund.

2.3 Normen en standaarden

Nr.	Standaard/norm	Bronnen/referenties
A1	De ICT Prestatie dient op de VeRA referentiecomponenten geplot te worden. Voor die referentiecomponenten die geraakt worden dient de ICT Prestatie tenminste de bij de referentiecomponent(en) gespecificeerde functionaliteit te bieden.	VeRA referentiecomponenten: veraonline.nl/index.php/Overzicht_referentiecomponenten
A2	Voor de ICT Prestatie is de VeRA kader stellend. De ICT Prestatie voldoet aan de visie en principes uit de VeRA.	VeRA visie en principes: veraonline.nl/index.php/Algemeen1

2.4 Tip

1. Neem in het programma van eisen en/of de Overeenkomst de naam en de beschrijvingen van de VeRA referentiecomponent(en) op.
2. De VeRA kaders en principes kunnen voor de specifieke uitvraag van Opdrachtgever worden vertaald en gedetailleerd in het programma van eisen.

3 Interoperabiliteit

3.1 Doel

Veiligheidsregio's maken gebruik van systemen van meerdere leveranciers. Ze willen voor een efficiënte uitvoering en dienstverlening informatie delen en werken in ketens samen met andere (overheids-) partijen. Gevolg is dat Veiligheidsregio's in staat moeten zijn om gegevens tussen verschillende systemen uit te kunnen wisselen. Goede, veilige en betrouwbare koppelingen zijn hiervoor noodzakelijk. Het gebruik van open standaarden voor interoperabiliteit zorgt voor inpasbaarheid van ICT Prestaties binnen het Applicatielandschap van Veiligheidsregio's. Dit leidt voor Veiligheidsregio's tot meer samenhang in het Applicatielandschap, grotere flexibiliteit in informatievoorziening en meer keuzevrijheid ten aanzien van software. Tevens zorgt het gebruik van standaarden voor het voorkomen van maatwerkkoppelingen en extra werkzaamheden die daaraan verbonden zijn.

3.2 Reikwijdte

Voor interoperabiliteit zijn standaarden per wet bepaald, evenals open standaarden die op de pas-toe-of-leg-uit lijst staan. Daarbij zijn er specifieke standaarden die gelden voor het Veiligheidsregio domein. Een deel van de standaarden specifiek voor het Veiligheidsregio domein betreft een nadere uitwerking van een meer generieke wettelijke dan wel open standaard. Daar waar die situatie zich voordoet dient aan de specifieke Veiligheidsregio eis voldaan te worden. Hiermee wordt invulling gegeven aan de verplichting uit de meer generieke open standaard.

De reikwijdte voor de toe te passen standaarden en normen is in twee delen gesplitst:

- Deel A betreft de specifieke standaarden voor het Veiligheidsregio domein en geldt voor dat deel van de ICT Prestatie dat binnen (delen van) het functionele werkingsgebied binnen het VeRA applicatielandschap valt;
- Deel B betreft de generieke standaarden en geldt voor de gehele ICT Prestatie.

3.3 Normen en standaarden

Nr.	Standaard/norm	Bronnen/referenties
B1	Deel A: Het betreffende deel van de ICT Prestatie voldoet aan alle verplichte standaarden (eindproduct en halffabricaat standaarden) van de bijbehorende VeRA referentiecomponent(en).	Voor de VeRA Referentiecomponenten: veraonline.nl/index.php/Overzicht_referentiecomponenten. Voor de verplichte standaarden en standaard bestekteksten: softwarecatalogusvr.nl/inkoopondersteuning.
B2	Deel B: Het betreffende deel van de ICT Prestatie voldoet aan de wettelijke standaarden, de open standaarden van de Pas-toe-of-leg-uit-lijst en de landelijke Veiligheidsregio standaarden voor zover het werkingsgebied van deze standaarden overeenkomt met het organisatorische of functionele werkingsgebied van het betreffende deel van de ICT Prestatie.	Open standaarden: forumstandaardisatie.nl/open-standaarden Landelijke Veiligheidsregio standaarden: veraonline.nl

3.4 Tips

1. Aan Opdrachtgevers wordt aangeraden om in het bestek op te nemen welke standaarden in ieder geval van toepassing zijn (verplichte standaarden). Zie zowel VeRA Online als de Veiligheidsregio softwarecatalogus. Daarnaast worden Opdrachtgevers aangeraden om te kijken welke standaarden vanuit VeRA Online aanbevolen worden. Beoordeel per aanbevolen standaard of je deze van toepassing wilt verklaren (conform GIBIT artikel 6.1 ii). Voor het van toepassing verklaren dient de standaard expliciet opgenomen te worden in het bestek.
2. Naast verplichte open standaarden zijn er ook aanbevolen standaarden op de lijst standaarden bij het Forum Standaardisatie: forumstandaardisatie.nl/open-standaarden/lijst/aanbevolen. Deze standaarden zijn niet verplicht om toe te passen, maar worden wel geadviseerd om te gebruiken voor een betreffend functioneel werkingsgebied. Opdrachtgevers worden aangeraden om in hun bestekduidelijk aan te geven welke van die aanbevolen standaarden ook verplicht worden gesteld (dit is conform GIBIT artikel 6.1 ii).
3. Conform GIBIT artikel 6.2 en 6.3 dient Leverancier preventieve testen uit te voeren op de verplichte standaarden. Indien een testinstrument beschikbaar is, staat dit bij de betreffende norm vermeld en wordt de Leverancier geacht deze test uit te voeren en een positieve uitslag aan Opdrachtgever te overleggen. Indien er geen testinstrument beschikbaar is, dan vervalt de verplichting om hieraan te voldoen.

4 Informatiebeveiliging en Privacy

4.1 Doel

Veiligheidsregio's verwerken veel informatie, waarvan een deel zeer (privacy)gevoelig is en extra beschermd dient te worden. Voor een groot deel van die informatieverwerking wordt gebruik gemaakt van ICT-producten en diensten van derden, waarmee goede afspraken moeten worden gemaakt over beveiliging en het waarborgen van privacy.
Informatiebeveiliging is het proces van vaststellen van de vereiste betrouwbaarheid van informatiesystemen in termen van beschikbaarheid, integriteit en vertrouwelijkheid (BIV) alsmede het treffen, onderhouden en controleren van een samenhangend pakket van bijbehorende beveiligingsmaatregelen. De betrouwbaarheid van een informatiesysteem is de verzamelterm voor de begrippen beschikbaarheid, integriteit en vertrouwelijkheid.
Betrouwbare informatiesystemen dragen bij aan het verlagen van risico's en vergroten van de weerbaarheid van de bedrijfsvoeringsprocessen van de veiligheidsregio.
verwerken veel persoonsgegevens. Vaak is het daarom nodig met leveranciers een verwerkersovereenkomst af te sluiten. Daartoe is een standaard verwerkersovereenkomst opgesteld. Dit document wordt gebruikt als aanvulling op een hoofdovereenkomst om nadere afspraken te maken over de omgang met persoonsgegevens.

4.2 Reikwijdte

Ten aanzien van informatiebeveiliging zijn er landelijk vastgestelde normen en standaarden. Sinds 1 januari 2019 is de Baseline Informatiebeveiliging Overheid (BIO) beschikbaar. 2019 was een overgangsjaar en vanaf 1 januari 2020 is de voor de hele overheid BIO de standaard.
Naast de BIO zijn ook de beveiligingsstandaarden van toepassing die vallen binnen de open standaarden. Zie het hoofdstuk Interoperabiliteit voor deze standaarden.

4.3 Normen en standaarden

Nr.	Standaard/norm	Bronnen/referenties
C1	De ICT Prestatie dient de functionele en technische mogelijkheden te hebben zodat de Opdrachtgever kan voldoen aan de Baseline Informatiebeveiliging Overheid (BIO).	De BIO: bio-overheid.nl

4.4 Tips

1. Om de implementatie van de BIO te ondersteunen, zijn door de IBD (Informatiebeveiligingsdienst voor gemeenten) producten ontwikkeld op operationeel niveau. Deze kennisproducten zijn beschikbaar opinformatiebeveiligingsdienst.nl/kennisproducten-ibd.
   Bewerkbare versies van de operationele producten zijn als download beschikbaar op de IBD-community (hiervoor is registratie noodzakelijk).
2. Bij de aanschaf van een (nieuw) informatiesysteem, wordt in de BIO voorgesteld om een baselinetoets BIO op te laten stellen door de proceseigenaar/ opdrachtgever. De vragenlijst vormt dan input voor de eventueel te nemen additionele beveiligingsmaatregelen, welke in de in de aanbestedingsdocumentatie nader dienen te worden uitgewerkt in eisen aan de leverancier. Dit kan bijvoorbeeld door middel van een aanvullende diepgaande risicoanalyse. De baselinetoets BIO bevat ook vragen om vast te kunnen stellen of er persoonsgegevens worden verwerkt en zo ja of er dan ook een DPIA nodig is. De Baseline BIO is te vinden op informatiebeveiligingsdienst.nl/product/baseline-informatiebeveiliging-overheid-bio.
3. Om de implementatie van beveiligingstandaarden te ondersteunen die op de lijst open standaarden van het Forum Standaardisatie (pas-toe-of-leg-uit lijst) staan, ontwikkelt de IBD regelmatig factsheets voor betreffende open standaarden (zoals, TLS, DNSSEC, SPF/DKIM/DMARC, DANE en STARTTLS). Deze factsheets zijn als download beschikbaar op informatiebeveiligingsdienst.nl/producten.
   Zie ook het hoofdstuk Interoperabiliteit waarin is aangegeven op welke wijze deze standaarden als vereist zijn geborgd en op welke wijze deze standaarden expliciet opgenomen kunnen worden in het bestek.
4. De bruikbaarheid van verschillende normen op het gebied van informatiebeveiliging in relatie tot de beveiligingsbehoeften van gemeenten wordt toegelicht in de Factsheet Assurance. Deze factsheet is als download beschikbaar op informatiebeveiligingsdienst.nl/product/factsheet-assurance.
5. Sinds 25 mei 2018 is de Algemene Verordening Gegevensbescherming (AVG) van toepassing. Artikel 25 van de AVG betreft de verplichting bij het verwerken van persoonsgegevens dat al bij het ontwerpen van de wijze van de verwerking, rekening gehouden dient te worden met het vereiste niveau van gegevensbescherming (‘Privacy by design’ of ‘Gegevensbescherming door ontwerp’). Indien in de opdracht gevraagd wordt te komen tot ontwikkeling van Programmatuur, dan wel het ontwikkelen van een aanvulling op bestaande Programmatuur, dan kan de Opdrachtgever in het programma van eisen opnemen dat reeds aan de verplichting voor ‘Privacy by design’ wordt voldaan.
6. In het kader van de AVG is door de vakgroep informatieveiligheid een model verwerkersovereenkomst opgesteld. Door gebruik te maken van deze model overeenkomst worden vanuit Veiligheidsregio’s op uniforme wijze de afspraken rondom de verwerking van persoonsgegevens geregeld.
7. Op internet.nl kan een check uitgevoerd worden om te kijken of voldaan wordt aan de juiste internetbeveiligingsstandaarden.

5 Dataportabiliteit

5.1 Doel

Veiligheidsregio's hebben de beschikking over veel data. Deze data is nodig om taken en diensten te verrichten. Vaak ligt deze data opgeslagen in ICT Prestaties van leveranciers, waar ook verwerking en creatie van data kan plaatsvinden. Het doel van dataportabiliteit is zorgen dat Opdrachtgever altijd toegang heeft tot de eigen data en deze betekenisvol kan overzetten naar andere systemen. Dataportabiliteit is de mogelijkheid eigen gegevens geautomatiseerd uit een informatiesysteem naar een ander systeem te kunnen verhuizen. Daar waar interoperabiliteit gaat over samenwerking en koppelingen tussen systemen gaat dataportabiliteit over het eruit kunnen halen van gegevens (exporteren) en zonder verlies van betekenis overzetten (migreren/importeren) ervan naar een ander systeem of platform. Dataportabiliteit is noodzakelijk voor het op lange termijn beschikbaar houden van ICT functionaliteiten, meer regie en bescherming van eigen gegevens en het makkelijker kunnen wisselen van leverancier en/of systeem.

5.2 Reikwijdte

Dataportabiliteit heeft zowel betrekking op de inhoud (waarden) van de data als op de bijbehorende metadata over de structuur en betekenis van die gegevens.
Het geautomatiseerd omzetten hiervan dient dit in een gangbaar formaat te gebeuren.
De metadata omvat tenminste:

1. De beschrijving van de betekenis van entiteiten, relaties, attributen, datatype en waardenbereik;
2. Het technische formaat.

5.3 Normen en standaarden

Nr.	Standaard/norm	Bronnen/referenties
D1	Dataportabiliteit moet mogelijk zijn voor de inhoud (waarden) van de data in de ICT Prestatie alsmede de bijbehorende metadata bestaande uit ten minste de beschrijving van de betekenis van entiteiten, relaties, attributen en waardenbereik	
D2	Het technische formaat voor dataportabiliteit dient bij voorkeur conform de XML of JSON standaarden. Indien een ander gangbaar technisch dataformaat wordt gebruikt dient de meta-informatie afzonderlijk gedocumenteerd te worden.	XML: w3.org/XML JSON: www.ecma-international.org/publications/files/ECMA-ST/ECMA-404.pdf (PDF)
D3	Opdrachtgever dient te kunnen beschikken over alle gegevens (buiten het aan te besteden systeem om). Toegang tot de data is mogelijk via open standaarden.	

Er wordt documentatie meegeleverd over het datamodel zodat het mogelijk is de gegevens op de juiste wijze te interpreteren.

5.4 Tips

1. Om dataportabiliteit te borgen voor de ICT Prestatie kan de volgende eis worden toegevoegd aan het bestek:
   “Leverancier geeft de specificaties voor dataportabiliteit. Deze specificaties voor dataportabiliteit bevatten voor de export én import van data tenminste:
   a. De beschrijving van betekenis van de data van entiteit, attributen en waardebereik;
   b. De beschrijving van betekenis en relaties (kardinaliteit) tussen gegevens;
   c. Het formaat waarin data kan worden geëxporteerd/geïmporteerd;
   d. Welke gegevens en metadata wel en niet worden meegenomen en het formaat waarin dat plaatsvindt;
   e. De beschrijving van de import en exportfunctionaliteit die het softwareproduct ondersteunt;
   f. De data die niet in de import en export meegenomen wordt omdat deze geen eigendom is van Opdrachtgever;
   g. Opgave van de technische formaten die voor dataportabiliteit gebruikt worden.”
2. Indien de over te dragen datastructuur en betekenis overeenkomt met een bestaand semantisch informatiemodel en bijbehorende XML of JSON gegevens/berichtenstandaard kan daarvan gebruik worden gemaakt.
3. Vanaf 25 mei 2018 is de Algemene Verordening Gegevensbescherming (AVG) van toepassing. In de AVG is dataportabiliteit ook opgenomen. Artikel 20 van de AVG betreft de verplichting tot het waarborgen van het ‘Recht op overdraagbaarheid van gegevens’ oftewel ‘gegevensoverdraagbaarheid’.

6 Toegankelijkheid

6.1 Doel

In Nederland willen wij dat openbare voorzieningen toegankelijk zijn voor alle burgers. Niet alleen gebouwen en bijvoorbeeld het openbaar vervoer, maar ook overheidswebsites en -webapps. Daarom is digitale toegankelijkheid belangrijk én verplicht voor de (semi-)overheid.

6.2 Reikwijdte

Alle (semi-)overheidswebsites en -webapps moeten toegankelijk zijn.

6.3 Normen en standaarden

Nr.	Standaard/norm	Bronnen/referenties
E1	Europese standaard EN 301549 met WCAG 2.1 (niveau A en AA)	digitoegankelijk.nl en forumstandaardisatie.nl/standaard/digitoegankelijk-en-301-549-met-wcag-21

6.4 Tips

1. Op digitoegankelijk.nl staat aangegeven welke vereisten er zijn, ook ten aanzien van het publiceren van een toegankelijkheidsverklaring.
2. Sinds 23 december 2018 is WCAG Update 2.1 verplicht. Meer informatie kan gevonden worden op digitoegankelijk.nl/actueel/nieuws/2018/11/1/wcag-2.1-update-vanaf-23-december-verplicht.
3. De verplichting geldt nu voor webgebaseerde producten en diensten (websites en webapps). De mogelijkheid bestaat voor Opdrachtgever om deze ook van toepassing te verklaren op digitale documenten die niet online worden aangeboden, voor mobiele applicaties (apps) en voor interne systemen. Dit dient de Opdrachtgever in het bestek te specificeren en eisen.

7 Archivering

7.1 Doel

Archivering heeft tot doel het zorgdragen dat gegevens duurzaam beschikbaar blijven, zodat het handelen van Veiligheidsregio's (publiek)verantwoord kan worden. Hiertoe dienen archiefbescheiden in geordende en toegankelijke staat te zijn.
Voor een goede vindbaarheid en archivering van informatie en uitwisseling van informatie tussen overheden is metadatering van (digitale) informatie noodzakelijk. Metadata geven informatie over Veiligheidsregio stukken. In metadata is informatie vastgelegd over de inhoud, context, structuur, vorm en het beheer van stukken door de tijd heen.
Veiligheidsregio's zijn op grond van de Archiefregeling verplicht een overzicht vast te stellen, waarin ze aangeven welke metadata voor de eigen organisatie minimaal nodig zijn en hoe deze worden vastgelegd.

7.2 Reikwijdte

Voor archivering staat de Archiefregeling centraal (wetten.overheid.nl/BWBR0027041/2014-01-01), die op haar beurt op het Archiefbesluit 1995 (wetten.overheid.nl/BWBR0007748/2013-01-01) en de Archiefwet (wetten.overheid.nl/BWBR0007376/2018-07-28) is gebaseerd. De Archiefregeling schrijft voor dat Veiligheidsregio's moeten beschikken over een kwaliteitssysteem en een metadateringsschema. De functionaliteiten van ICT-systemen moeten voldoen aan deze eisen. Overigens: Archiefwet en Archiefregeling spreken over archiefbescheiden. Daarmee wordt bedoeld: alle informatie die door een Veiligheidsregio ontvangen, gecreëerd en verwerkt wordt.

7.3 Normen en standaarden

Nr.	Standaard/norm	Bronnen/referenties
F1	Kwaliteitssysteem voor beheer van archiefbescheiden: Kwaliteitssys-teem Informatiebeheer Decentrale Overheden (KIDO)	Archiefregeling, artikel 16 NEN-ISO 15489 is de norm, KIDO omvat de uitwerking daarvan
F2	Metadateringsschema: TMLO	Archiefregeling, artikel 19 NEN-ISO 23081 is het voorschrift. TMLO is de uitwerking daarvan voor lagere overheden.
F3	Selectielijst gemeenten en interge-meentelijke organen 2017	vng.nl/onderwerpenindex/dienstverlening-en-informatiebeleid/archieven/nieuws/selectielijst-gemeenten-en-intergemeentelijke-organen-2017

F4	De ICT Prestatie is geschikt om conform NEN 2082 te archiveren	noraonline.nl/wiki/NEN_2082

7.4 Tips

1. Het kwaliteitssysteem is nader uitgewerkt in project KIDO (Kwaliteit Informatiebeheer Decentrale Overheden): vng.nl/onderwerpenindex/dienstverlening-en-informatiebeleid/dienstverlening-aan-inwoners-en-ondernemers/nieuws/handreiking-kwaliteitssysteem-informatiebeheer-beschikbaar.
2. Meer informatie over het Toepassingsprofiel Metadata Lokale Overheden (TMLO) via nationaalarchief.nl/archiveren/kennisbank/tmlo. In 2020 wordt het TMLO verder doorontwikkeld en samengevoegd met het Toepassingsprofiel Metagegevens Rijksoverheid (TP Rijk).
3. Bij de selectielijst is de SelectTool ontwikkeld. Hiermee kunnen regels uit de selectielijst eenvoudig gekoppeld worden aan een zaaktypecatalogus. De tool is te vinden via vng.nl/onderwerpenindex/dienstverlening-en-informatiebeleid/archieven/nieuws/selectielijst-gemeenten-en-intergemeentelijke-organen-2017.

8 Generieke Digitale Infrastructuur (GDI) en de basisregistraties

8.1 Doel

De maatschappij verandert steeds meer in een informatie- en netwerksamenleving. De overheid moet daarop aansluiten. Overheidsbrede voorzieningen bieden een gemeenschappelijke basis om de dienstverlening te verbeteren, in te spelen op de veranderingen in de maatschappij en effectiever de mogelijkheden van nieuwe technologie te benutten. Het doel is te borgen dat de gemeenschappelijke voorzieningen (her)gebruikt worden. Deze gemeenschappelijke voorzieningen betreffen de Generieke Digitale Infrastructuur (GDI) en de basisregistraties.

8.2 Reikwijdte

ICT Prestaties moeten daar waar van toepassing aansluiten op en gebruik maken van bestaande voorzieningen van de GDI en de basisregistraties.
De GDI bestaat uit standaarden, producten en voorzieningen die gezamenlijk gebruikt worden door (alle) overheden, vele publieke organisaties en in een aantal gevallen ook door private partijen. De GDI is een onmisbaar deel van de (digitale) basisvoorzieningen waarmee organisaties hun primaire processen inrichten.
Er zijn tien basisregistraties. Een basisregistratie is een door de overheid officieel aangewezen registratie met gegevens die door alle overheidsinstellingen verplicht worden gebruikt bij de uitvoering van publiekrechtelijke taken. Dit kan gaan om uitrukkende hulpdiensten, het efficiënt vaststellen van het recht op uitkering of het toetsen van vergunningaanvragen. Bij het gebruik van de gegevens is de privacy van de burger gewaarborgd.

8.3 Normen en standaarden

Nr.	Standaard/norm	Bronnen/referenties
G1	Aansluiten op voorzieningen uit de GDI	Het overzicht van de GDI is gegeven op vngrealisatie.nl/onderwerpen/generieke-digitale-infrastructuur-gdi.
G2	Aansluiten op basisregistraties	Het overzicht van de basisregistraties en meer informatie daarover: digitaleoverheid.nl/dossiers/basisregistraties.

8.4 Tips

1. De landelijke infrastructuur (GDI) en de basisregistraties zijn continue in ontwikkeling. Houd bij verwerving van in te kopen ICT Prestaties rekening met nieuwe mogelijkheden, kaders en eisen. Opdrachtgevers wordt aangeraden om in hun bestek heel duidelijk aan te geven op welke van de landelijke voorzieningen van GDI en basisregistraties aangesloten moet worden en welke standaarden daarvoor gebruikt dienen te worden.

9 Documentatie

9.1 Doel

Goede documentatie is noodzakelijk om een ICT Prestatie optimaal te implementeren, in te passen in het Applicatielandschap, te gebruiken binnen een bedrijfsproces, keten en/of in dienstverlening en te beheren en te onderhouden.

9.2 Reikwijdte

Voor de gehele ICT Prestatie gelden de vereisten ten aanzien van documentatie zoals opgenomen in GIBIT artikel 11. GIBIT artikel 11.1 geeft aan welke inhoudelijke eisen gelden ten aanzien van documentatie. In artikel 11.1 lid v wordt expliciet aangegeven dat een uitwerking van het vereiste is opgenomen in de Veiligheidsregio ICT-kwaliteitsnormen. Dit laat onverlet dat de vereisten zoals opgenomen in artikel 11.1. lid i t/m iv te allen tijde gelden voor de gehele ICT Prestatie.
GIBIT artikel 11.1 lid v geeft aan dat de documentatie zodanig zal zijn en blijven dat zij geschikt is om op basis hiervan de ICT Prestatie adequaat te kunnen beheren en te kunnen inpassen in het Applicatielandschap.

9.3 Normen en standaarden

Nr.	Standaard/norm	Bronnen/referenties
H1	Leverancier dient documentatie op te leveren waarbij de inhoud, diepgang en actualiteit per product/pakketversie omvat minimaal de volgende informatie: 1. Afdekking beleidsthema en functioneel werkingsgebied 2. Functionele beschrijving 3. Ondersteunde standaarden inclusief compliance aanduiding(en) en testrapport	n.v.t.

9.4 Tip

1. Opdrachtgever wordt aanbevolen om eventuele aanvullende eisen ten aanzien van documentatie op te nemen in het Programma van Eisen.

10 E-facturering

10.1 Doel

Door e-facturering wordt het proces van facturering efficiënter en beter. Handmatige verwerking is daarmee verleden tijd. Een e-factuur is een gestructureerd, digitaal bestand (maar geen pdf) waarbij alle gegevens altijd op een vaste plek in het bestand staan en hun eigen betekenis hebben. Een e-factuur kan vanuit het ene geautomatiseerde systeem elektronisch worden verwerkt in het andere systeem.

10.2 Reikwijdte

Alle aanbestedende diensten zijn gehouden aan de verplichting in de Aanbestedingswet om per 18 april 2019 e-facturen te kunnen ontvangen en verwerken. Daar waar de GIBIT van toepassing is en waar elektronische facturen zijn overeengekomen, dient dit aan de hier vermelde standaarden te voldoen.

10.3 Normen en standaarden

Nr.	Standaard/norm	Bronnen/referenties
I1	UBL-SimplerInvoicing 1.1	simplerinvoicing.org/download-documenten/

10.4 Tips

1. GIBIT artikel 9.5 geeft aan dat – tenzij anders overeengekomen – de factuur elektronisch verzonden moet worden. Zorg als Opdrachtgever er voor dat u deze elektronische facturen ook kunt ontvangen en verwerken.
2. De verplichting in de Aanbestedingswetgeving houdt concreet in dat de Rijksoverheid, de decentrale overheden en alle andere aanbestedingsplichtige organisaties per 18 april 2019 e-facturen moeten kunnen ontvangen en verwerken. Voor ondersteuning bij de implementatie van e-factureren bij medeoverheden is het programmabureau e-factureren ingericht bij PIANOo, zie pianoo.nl/themas/elektronisch-factureren.