Veiligheidsregio ICT-kwaliteitsnormen

Behorende bij GIBIT 2016 en GIBIT 2020 (Gemeentelijke Inkoopvoorwaarden bij IT)

Versie: Definitief, december 2023

Nederlands Instituut Publieke Veiligheid
Postbus 7010
6801 HA Arnhem
Kemperbergerweg 783, Arnhem
www.nipv.nl
info@nipv.nl
026 355 24 00

Colofon

Titel:	Veiligheidsregio ICT-kwaliteitsnormen
Datum:	1 december 2023
Status:	Definitief
Versie:	2023

1 Inleiding

In november 2020 is door de VNG een bijgewerkte versie van de Gemeentelijke Inkoopvoorwaarden bij IT(GIBIT) vastgesteld. De GIBIT is een set uniforme en gestandaardiseerde inkoopvoorwaarden die gemeenten en gemeentelijke samenwerkingsverbanden kunnen gebruiken bij de verwerving van ICT-producten of -diensten. Een nadere specificatie van het toepassensgebied van de GIBIT is beschreven in de toelichting bij de voorwaarden.

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.

Noot: de inleiding bij deze versie van de Veiligheidsregio ICT-kwaliteitsnormen sluit inhoudelijk aan bij de 2020-versie van de GIBIT. Deze versie van de kwaliteitsnormen geldt echter óók voor lopende en nieuwe contracten die zijn of worden afgesloten op basis van de GIBIT 2016. De relatie tussen de Veiligheidsregio ICT-kwaliteitsnormen en de GIBIT 2016 is beschreven in artikelen 6.1 (Overeengekomen gebruik), 8.9 (Preventief en Innovatief Onderhoud), en 10.1 (Garanties).

Voor opdrachtgevers is het van belang dat een te verwerven ICT-product of -dienst aansluit bij hun verdere Applicatielandschap. Om deze aansluiting te realiseren is het veelal nodig dat de ICT Prestatie voldoet aan bepaalde normen en standaarden, bijvoorbeeld op gebied van interoperabiliteit of beveiliging.

In de Veiligheidsregio ICT-kwaliteitsnormen is een aantal voor veiligheidsregio's belangrijke normen en standaarden beschreven. **Het is van belang bij een verwervingstraject expliciet op te nemen dat de Veiligheidsregio ICT-kwaliteitsnormen van toepassing zijn in plaats van de Gemeentelijke ICT-kwaliteitsnormen bij gebruik van de GIBIT binnen Veiligheidsregio's.**

Dit document beschrijft allereerst welke normen en standaarden onderdeel uitmaken van de Veiligheidsregio ICT-kwaliteitsnormen. Tevens wordt toegelicht welke eisen gelden voor opname in dit document en op welke wijze de Veiligheidsregio ICT-kwaliteitsnormen onderhouden en gebruikt kunnen worden. Begrippen die in de GIBIT gedefinieerd zijn, zijn met een hoofdletter aangeduid.
De Veiligheidsregio ICT-kwaliteitsnormen wordt gepubliceerd door het Nederlands Instituut Publieke Veiligheid (NIPV) op softwarecatalogusvr.nl/inkoopondersteuning en wordt incidenteel voorzien van bijgewerkte normen en standaarden voor ICT-producten en diensten.

1.1 Aanbevelingen bij gebruik van de Veiligheidsregio ICT-kwaliteitsnormen

De Veiligheidsregio ICT-kwaliteitsnormen zijn in de eerste plaats bedoeld als vangnet. Bij het ontbreken van afwijkende afspraken moet leverancier ervoor zorgen dat de ICT Prestatie voldoet aan de daarvoor relevante normen en standaarden (GIBIT-artikel 6.1 sub i).
Om een zo passend mogelijk aanbod van leveranciers te krijgen, is het echter aan te bevelen tijdens het voorbereidingsproces van een verwervingstraject de kwaliteitsnormen nader te bekijken en te specificeren. Hiertoe kunnen vier aanbevelingen worden gedaan:

1. *Neem relevante kwaliteitsnormen expliciet op in de opdrachtdocumentatie*
   Hierdoor is, in gevallen waar als onderdeel van de opdracht onderhoud wordt gepleegd, het bijwerken naar nieuwe versies van normen of standaarden gewaarborgd (GIBIT-artikel 8.10 sub ii).
2. *Geef relevante kwaliteitsnormen in de opdrachtdocumentatie nader invulling*
   Zo is het voor zowel opdrachtgever als leverancier duidelijk aan welke normen (delen van) de ICT Prestatie precies moet voldoen. Bovendien worden onnodige kosten vermeden door implementatie van (delen van) normen of standaarden waaraan geen behoefte is. Nadere specificatie is met name van belang voor toepassingsafhankelijke normen zoals *Interoperabiliteit* (toepassen standaarden hangen af van het toepassingsgebied van de ICT Prestatie) en *Informatiebeveiliging en Privacy* (beveiligingsniveau is onder andere afhankelijk van gevoeligheid van met de ICT Prestatie verwerkte gegevens).
3. *Betrek (domein)experts bij het vaststellen van de relevantie van kwaliteitsnormen*
   Deze aanbeveling ligt in het verlengde van de vorige. Het nader invullen van aantal kwaliteitsnormen vereist veelal specialistische kennis en ervaring. Dit zal bijvoorbeeld vaak gelden voor normen ten aanzien van *Architectuur, Interoperabiliteit, Informatiebeveiliging* en *Archivering*.
4. *Gebruik de GIBIT-overeenkomstengenerator om een (concept)overeenkomst te generen*
   In de GIBIT-overeenkomstengenerator is ruimte om met de GIBIT en de Gemeentelijke ICT-kwaliteitsnormen als basis een overeenkomst te genereren die op de GIBIT of kwaliteitsnormen nadere of afwijkende afspraken omvat. De overeenkomstengenerator is te vinden op overeenkomsten.gibit.nl.

1.2 Reikwijdte Veiligheidsregio ICT-kwaliteitsnormen

De Veiligheidsregio ICT-kwaliteitsnormen betreffen normen en standaarden waaraan verplicht moet worden voldaan. De verplichting kan volgen uit:

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

Iedere norm en standaard die in de Veiligheidsregio ICT-kwaliteitsnormen wordt opgenomen is vastgesteld. Standaarden of versies van standaarden die nog in ontwikkeling zijn kunnen dus geen onderdeel zijn van de Veiligheidsregio ICT-kwaliteitsnormen.
Het vaststellingsproces kan per norm verschillen, dit is mede afhankelijk van de beheerder van en governance-structuur bij de betreffende norm. Voor wettelijke normen geldt de wetgever als vaststeller. Landelijk vastgestelde open standaarden worden vastgesteld onder regie van het Forum Standaardisatie. En specifiek Veiligheidsregio standaarden worden

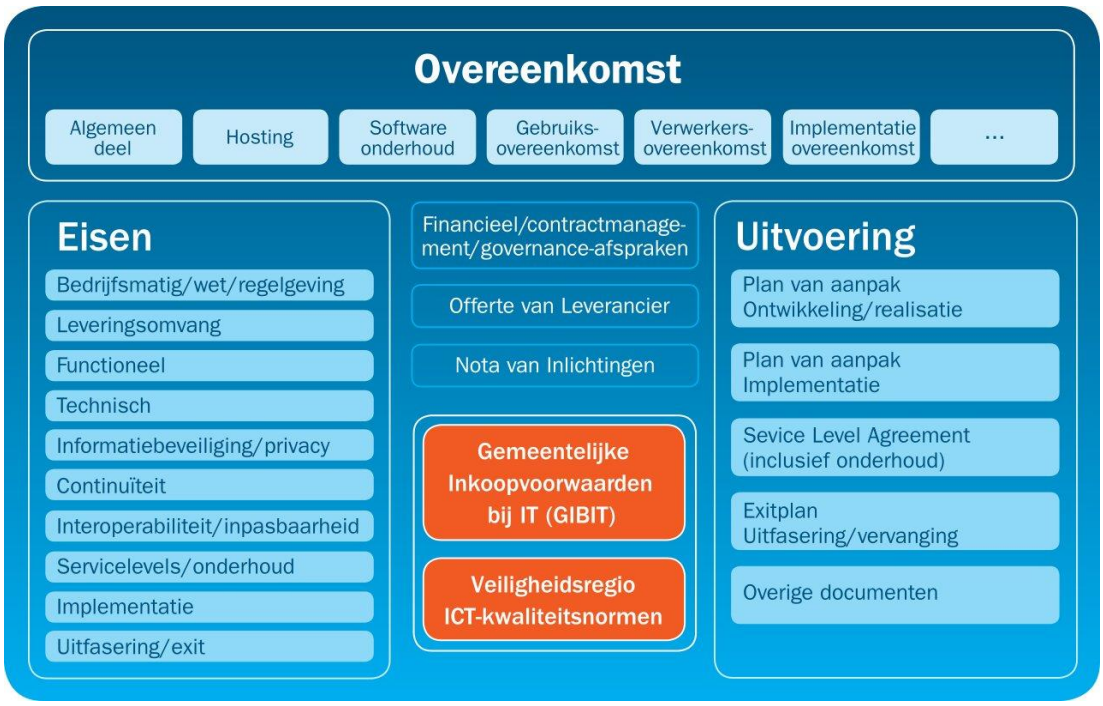
onder regie van de Architectuurboard van de Veiligheidsregio's vastgesteld. In alle gevallen is een standaardisatieproces ingericht waarbij Veiligheidsregio's nauw betrokken zijn en mede bepalen hoe de norm of standaard eruit gaat zien. In veel gevallen spelen ook ICT leveranciers een rol in het vaststellingsproces.
Enkele normen zoals die voor *Documentatie* en *Dataportabiliteit* wijken van het bovenstaande af. Deze zijn niet gebaseerd op landelijke afspraken, maar op internationale standaarden of binnen de ICT zeer gangbare normen of formaten.
De Veiligheidsregio ICT-kwaliteitsnormen hebben betrekking op de volgende ICT-kwaliteitsgebieden:

- Architectuur
- Interoperabiliteit
- Informatiebeveiliging en Privacy
- Dataportabiliteit
- Digitale toegankelijkheid
- Archivering
- Infrastructuur: generieke digitale infrastructuur (GDI) en de basisregistraties
- Documentatie
- E-facturering

In dit document zijn voor ieder bovengenoemd ICT-kwaliteitsgebied het doel, de reikwijdte en de bijbehorende standaarden of normen beschreven.

1.3 Toepassing van de Veiligheidsregio ICT-kwaliteitsnormen

Onderstaande figuur toont een schematisch overzicht tussen de Overeenkomst, de onderliggende GIBIT-voorwaarden met Veiligheidsregio ICT-kwaliteitsnormen en de eisen die door Opdrachtgever op verschillende gebieden gesteld kunnen worden.



De Veiligheidsregio ICT-kwaliteitsnormen zijn van toepassing als de GIBIT van toepassing verklaard is. Dit geldt zowel in de situatie dat een Overeenkomst wordt gesloten waarop de GIBIT van toepassing is verklaard, als wanneer een Opdrachtgever tijdens 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 de GIBIT geciteerd wordt). In de laatste alinea volgt nog de aanvulling hoe om te gaan met nieuwe versies van de Veiligheidsregio ICT-kwaliteitsnormen.**

In GIBIT-artikel 6.1(i) is beschreven dat het voldoen aan de Gemeentelijke ICT-kwaliteitsnormen onderdeel is van het 'Overeengekomen gebruik'. Hieruit volgt dat Leverancier geacht wordt bekend te zijn met (de inhoud van) de Gemeentelijke ICT-kwaliteitsnormen.
Concreet betekent artikel 6.1 dat de ICT Prestatie ("de te leveren goederen en diensten") moet voldoen aan de Gemeentelijke ICT-kwaliteitsnormen. Hierop zijn echter twee beperkingen van toepassing.

1. **Bereik:** er hoeft alleen te worden voldaan aan in Gemeentelijke ICT-kwaliteitsnormen opgenomen interoperabiliteitseisen, normen en standaarden *voor zover die relevant zijn voor de functie of gelden voor het werkingsgebied van de ICT Prestatie.*
2. **Tijd:** er hoeft alleen te worden voldaan aan die interoperabiliteitseisen, normen en standaarden *die tijdens het sluiten van de Overeenkomst voorgeschreven waren* (hoewel het voldoen aan bij nieuwe versies onderdeel kan zijn van afspraken over Onderhoud).

De in de GIBIT voorgeschreven normen en standaarden zijn minimumeisen.
GIBIT-artikel 6.1 ii creëert voor Opdrachtgevers dan ook de mogelijkheid om van Leveranciers te vragen te voldoen aan aanvullende normen en standaarden - bijvoorbeeld de *verplichte* implementatie van een standaard die volgens de Gemeentelijke ICT-kwaliteitsnormen slechts een *aanbevolen* karakter heeft. Hierom moet door de Opdrachtgever wel expliciet in de Overeenkomst worden gevraagd.

GIBIT-artikelen 6.2 t/m 6.5 zien toe op het uitvoeren van (preventieve) testen van de ICT Prestatie ten aanzien van de geldende Gemeentelijke ICT-kwaliteitsnormen. Artikel 6.4 bepaalt dat tijdens de Acceptatieprocedure getoetst wordt of voldaan is aan de krachtens 6.1 toe te passen normen. Bij individuele normen binnen de Gemeentelijke ICT-kwaliteitsnormen is aangegeven welke testvoorzieningen beschikbaar en te gebruiken zijn.

Normen en standaarden kunnen tijdens de looptijd van een Overeenkomst veranderen. Van veel normen verschijnen immers regelmatig nieuwe of bijgewerkte versies. Om interoperabiliteit en het voldoen aan wetgeving tijdens de contractperiode te garanderen, is het noodzakelijk dat deze nieuwe versies binnen een redelijke termijn worden geïmplementeerd. Wat die redelijke termijn is, is niet in algemene zin te zeggen. Omdat de Gemeentelijke ICT-kwaliteitsnormen uitsluitend vastgestelde normen omvat, zijn aanpassingen echter vrijwel altijd ruim tevoren te voorzien. Bij vaststelling van (aangepaste) normen is bovendien vaak sprake van een overgangsperiode, zoals de periode tussen vaststelling en het daadwerkelijk ingaan in het geval van nieuwe wetgeving.

Om implementatie van nieuwe (versies van) normen en standaarden tijdens de looptijd van de overeenkomst te ondersteunen, is in GIBIT-artikel 8.10 sub iii bepaald dat het implementeren van nieuwe versies van normen en standaarden onderdeel is van het Onderhoud dat Leverancier uitvoert. Deze verplichting wordt beperkt tot die normen en standaarden waarvoor implementatie in de Overeenkomst expliciet en verplichtend is benoemd. Tegenover deze verplichting kan een vergoeding staan. GIBIT-artikel 8.1 nodigt Leverancier en Opdrachtgever uit hierover in de Overeenkomst afspraken vast te leggen. 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.

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/Visie_en_principes

2.4 Tips

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 drie 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.
- Deel C betreft de API-standaarden die horen bij de informatiekundige visie Common Ground en de architectuur van het VeRA Gegevenslandschap. Deze standaarden kunnen voor wat betreft hun functioneel werkingsgebied overlappen met standaarden uit delen A en B. Gedurende de transitie naar een gegevenslandschap kan het wenselijk zijn dat een informatiesysteem zowel de standaarden die horen bij A, B en C ondersteunt, zelfs als dat betekent dat door implementatie van functioneel gelijkaardige standaarden bepaalde functionaliteit dubbel wordt geïmplementeerd.

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
B3	Deel C: Tenzij Opdrachtgever anders bepaalt, voldoet het betreffende deel van de ICT Prestatie aan gemeentelijke API-standaarden, voor zover het werkingsgebied van deze standaarden overeenkomt met het organisatorische of functionele werkingsgebied van het betreffende deel van de ICT Prestatie.	Zie kopje ‘API-standaarden’ op: vng.nl/artikelen/overzicht-gemeentelijke-standaarden

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. Een overzicht van API-standaarden is te vinden op vng.nl/artikelen/overzicht-gemeentelijke-standaarden. Ten opzichte van de StUF-standaarden sluiten deze API-standaarden beter aan bij door softwareontwikkelaars gebruikte industriestandaarden. Bovendien zijn ze flexibeler toe te passen, en maken ze het mogelijk de uitgangspunten van de architectuur van het Bedrijfsinformatiemodel Veiligheidsregio (veraonline.nl/index.php/Bedrijfsinformatiemodel_Veiligheidsregio_(BIM)) en de thema architectuur common ground (Thema-architectuur Common Ground - GEMMA Online) toe te passen. Voor API's, als eerste die voor zaakgericht werken (ZGW API's), is een testvoorziening gerealiseerd waarmee kan worden beproefd of een implementatie van één of meer ZGW API's voldoet aan de bijbehorende specificaties. Deze testvoorziening is te vinden op api-test.nl.

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.

Veiligheidsregio's 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: informatiebeveiligingsdienst.nl/project/baseline-informatiebeveiliging-overheid

C2	De Informatiebeveiliging dient op de VeRA referentiecomponenten met name de SecurityReferentieArchitectuur, geplot te worden. Voor die referentiecomponenten die geraakt worden dient de Informatiebeveiliging tenminste aan de bij de referentiecomponent(en) gespecificeerde eisen te voldoen.	VeRA referentiecomponenten: veraonline.nl/index.php/Overzicht_referentiecomponenten

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 op informatiebeveiligingsdienst.nl/kennisproducten-ibd.
   Bewerkbare versies van de operationele producten zijn als download beschikbaar op de IBD-community (hiervoor is registratie noodzakelijk).
2. Hoewel niet gericht op VR's kan gebruik gemaakt worden van (delen van) de IRPA-tool die kan helpen te bepalen welke beveiligings- en privacy maatregelen moeten worden uitgevraagd. De tool is beschikbaar op https://www.informatiebeveiligingsdienst.nl/irpa-tool.
3. 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.
4. 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.
   Om te bepalen welke standaarden van toepassing zijn kunt u ook gebruik maken van de beslisboom (Beslisboom Open Standaarden | Forum Standaardisatie) van het Forum Standaardisatie.
   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.
5. 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.
6. 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.

7. 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.
8. 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 is een open formaat en sluit bij voorkeur aan bij de XML of JSON standaarden. Indien aan het bovenstaande niet voldaan kan worden en 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 waarborgen 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 waardenbereik;
   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. Er is geen wereldwijd algemeen geaccepteerde definitie van wat een ‘open (bestands)formaat’ is. De toelichting van het Forum Standaardisatie bij ‘open standaarden’ wordt gebruikt als leidraad bij het bepalen of sprake is van een open formaat: forumstandaardisatie.nl/open-standaarden/wat-zijn-open-standaarden.
4. 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 Digitale 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. Onder websites vallen ook intra- en extranetten en cloudapplicaties volgens de Europese definitie (zie https://www.digitoegankelijk.nl/wetgeving/specifieke-situaties/intranetten-extranetten-en-cloudapplicaties).

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. Voor de digitale toegankelijkheid is het in veel gevallen beter informatie als webpagina te publiceren dan als (Pdf-)bestand. Het Forum Standaardisatie heeft een handreiking gemaakt die helpt de meest passende publicatievorm te vinden: forumstandaardisatie.nl/thema/informatie-open-en-toegankelijk. Toch een Pdf-bestand publiceren? Dan wordt het gebruik van PDF/UA aanbevolen. Dit formaat is duurzaam en (mits correct opgemaakt) toegankelijk. Zie https://forumstandaardisatie.nl/open-standaarden/pdfua.
2. Op digitoegankelijk.nl/wetgeving/wat-verplicht staat aangegeven welke vereisten er zijn, ook ten aanzien van het publiceren van een toegankelijkheidsverklaring.
3. Het Tijdelijk besluit digitale toegankelijkheid overheid is per 1 juli 2018 in werking getreden in Nederland. In het besluit is bepaald dat websites en mobiele apps van overheidsinstanties op de volgende datums aan het besluit moeten voldoen:
    a. Op 23 september 2019 voor websites die zijn gepubliceerd vanaf 23 september 2018;
    b. Op 23 september 2020 voor websites die zijn gepubliceerd voor 23 september 2018;
    c. Op 23 juni 2021 voor mobiele applicaties.

4. De mogelijkheid bestaat voor Opdrachtgever om deze ook van toepassing te verklaren op voorzieningen die niet openbaar aangeboden worden, 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: Kwaliteitssysteem Informatiebeheer Decentrale Overheden (KIDO)	Archiefregeling, artikel 16 NEN-ISO 15489 is de norm, KIDO omvat de uitwerking daarvan
F2	Metadateringsschema: MDTO	Archiefregeling, artikel 19 NEN-ISO 23081 is het voorschrift. MDTO is de uitwerking daarvan voor lagere overheden.
F3	Selectielijst gemeenten en intergemeentelijke organen 2020	vng.nl/nieuws/selectielijst-2020-vastgesteld
F4	De ICT Prestatie is geschikt om conform NEN-ISO 16175-1:2020 te archiveren	noraonline.nl/wiki/NEN-ISO_16175-1

7.4 Tips

1. Het kwaliteitssysteem is nader uitgewerkt in project KIDO (Kwaliteit Informatiebeheer Decentrale Overheden): vng.nl/files/vng/nieuws_attachments/2016/handreikingkido.def.pdf.
2. Duurzaam Toegankelijke Overheidsinformatie' (MDTO) is de standaard voor metagegevens die in het kader van duurzame toegankelijkheid worden vastgelegd. Toelichting en het metadataschema zelf zijn beschikbaar via nationaalarchief.nl/archiveren/mdto. Meer informatie over het Toepassingsprofiel Metadata Lokale Overheden (TMLO) via nationaalarchief.nl/archiveren/kennisbank/tmlo.
3. Bij de selectielijst 2020 is een handreiking en SelectTool beschikbaar gesteld. Deze zijn beschikbaar via vng.nl/nieuws/selectielijst-2020-vastgesteld.
4. NEN-ISO 16175-1 beschrijft functionaliteit die binnen de Veiligheidsregio informatievoorziening beschikbaar moet zijn om de duurzame toegankelijkheid van informatie te waarborgen. De ICT Presentatie moet, als die 'archiefstukken' verwerkt, alleen of in combinatie met andere (eventueel al in het applicatielandschap van de gemeente) aanwezige componenten de in de norm verplichte functionaliteit kunnen leveren. Opdrachtgevers kunnen aan de hand van de norm bepalen hoe ze de hiervoor benodigde functionaliteit over individuele applicaties of componenten binnen het applicatielandschap verdelen. NEN-ISO 16175 is tegen betaling bij NEN verkrijgbaar.

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.
Het NIPV realiseert en beheert in opdracht van de Veiligheidsregio de landelijke voorzieningen. Naast applicaties (LCMS) zijn dit ook generieke infrastructuur voorzieningen (Verkeersplein/ landelijk koppelvlak).

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.
G3	Aansluiten op Veiligheidsregio brede infrastructuur voorzieningen (Landelijk koppelvlak - Verkeersplein).	Zie Informatievoorziening - Nederlands Instituut Publieke Veiligheid (nipv.nl)

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.
2. Bij het ontwikkelen van applicaties is Haven te gebruiken als standaard voor platform-onafhankelijke cloud hosting. Dit verhoogt de portabiliteit en vermindert beheerlast. Verdere informatie is te vinden op Haven - Homepage (commonground.nl).

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 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

Daar waar de GIBIT van toepassing is en waar elektronische facturen zijn overeengekomen, dienen deze aan de hier vermelde standaarden te voldoen.

10.3 Normen en standaarden

Nr.	Standaard/norm	Bronnen/referenties
I1	EN16931 en NLCIUS	forumstandaardisatie.nl/open-standaarden/nlcius

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. Met ingang van november 2018 zijn overheden op grond van de Europese richtlijn inzake e-factureren (EU/55/2014) verplicht bij overheidsopdrachten e-facturen te kunnen ontvangen en verwerken. Hiervoor is de Europese norm EN16931 ontwikkeld. NLCIUS is een aanvullende nationale specificatie op EN16931 voor toepassing in Nederland.
3. Voor het gestandaardiseerd, veilig en betrouwbaar uitwisselen van factuurgegevens is een internationale digitale infrastructuur en afsprakenstelsel ontwikkeld: Peppol. De Nederlandse Peppol-infrastructuur wordt namens de internationale stichting ‘OpenPeppol’ beheerd door de Nederlandse Peppolautoriteit (peppolautoriteit.nl).