

Tabblad 0 - Eisen en wensen Algemeen m.b.t. Hosting en Storage

Aanbesteding Hosting Belastingsamenwerking Gemeenten en Waterschappen Limburg



Bijlage D1 Algemeen

nr	Omschrijving eisen	Type eis	Voldoet de aangeboden oplossing?	Toelichting
ALG1	Algemeen			
ALGD1-01	De Dienstverlener is in staat tot het leveren van de huidige bij BsGW in gebruik zijnde software, zoals opgenomen in de bijlage P1 - Applicatieoverzicht, waar nodig inclusief het leveren van additionele licenties, abonnementen en support- en onderhoudscontracten, voor zover vrij verkrijgbaar in de markt.	Eis		
ALGD1-02	De voorgestelde oplossing is geschikt voor 200 medewerkers en is makkelijk op en af te schalen.	Eis		
ALGD1-03	Alle applicaties en ingerichte koppelingen in gebruik door de opdrachtgever dienen ondersteund te worden. Deze koppelingen zijn wezenlijk voor de werking van de applicaties. Zie bijlage P1 - Applicatieoverzicht en bijlage P4 - Overzicht verbindingen	Eis		
ALGD1-04	Applicaties zijn beschikbaar onafhankelijk van de fysieke locatie van de werkplek.	Eis		
ALGD1-05	De door Dienstverlener geleverde diensten en/of oplossingen voldoen gedurende de looptijd van de overeenkomst doorlopend aan de voor BsGW relevante vigerende wet- en regelgeving.	Eis		
ALGD1-06	De Dienstverlener dient gebruik te maken van binnen de EER (Europese Economische Ruimte) gesitueerde datacenters, waarbij de data van Opdrachtgever binnen de EER is opgeslagen.	Eis		

ALGD1-07	De Dienstverlener dient gebruik te maken van in Nederland gesitueerde datacenters, waarbij de data van Opdrachtgever in Nederland is opgeslagen.	Wens		
ALGD1-08	Dienstverlener dient toekomstige platformen / technieken (die BsGW wenst/eist in gebruik te nemen) te ondersteunen, ongeacht welke technieken en platformen dit zijn (bijvoorbeeld aansluiten op SaaS oplossingen van derden.) Hierbij is het uitgangspunt dat BsGW aansluit op GDI.	Eis		
ALGD1-09	Dienstverlener voert alle wijzigingen in de IT infrastructuur uit die nodig zijn om de afgesproken prestaties te leveren zonder additionele kosten in rekening te brengen.	Eis		

Tabblad 1 - Eisen en wensen Hosting en Storage

Aanbesteding Hosting Belastingsamenwerking Gemeenten en Waterschappen Limburg

Bijlage D1 Hosting en Storage



nr	Omschrijving eisen	Type eis	Voldoet de aanbode n	Toelichting
HOST	Hosting en Storage			
HOST-01	De Dienstverlener zorgt voor de levering van: <ul style="list-style-type: none"> - Standaard software (commercial off the shelf); - Open source software; - Cloud applicaties (SaaS, PaaS) en Application Hosting; - Licenties, software assurance, software abonnementen en bijbehorende voorwaarden en productdocumentatie; - Certificaten die benodigd zijn voor het functioneren van de betreffende applicaties; - Support en onderhoudscontracten op de software; - Patches en upgrades; - Software en oplossingen ten behoeve van koppelingen/integraties tussen applicaties. 	Eis		
HOST-02	De Dienstverlener voert het systeembeheer uit op de volgende platform services (servers) en rollen van BsGW: <ul style="list-style-type: none"> - Applicatieservers (Windows); - Web servers (IIS); - File services; - Printservers (alleen OS, printservices worden beheerd door externe leverancier) - Networking services (DNS, DHCP, DMZ, Firewalls, VPNs, Wireless network, Internetlijnen); - Microsoft infrastructuur services (Active Directory, Certificate Services, Key Management Services, etc.). <p>Zie bijlage N - BsGW platform (SOLL) v1.1</p>	Eis		

HOST-03	<p>De Dienstverlener zorgt ervoor dat alle platform services doorlopend zijn voorzien van de meest actuele versies van besturingssysteem software, patches en updates conform de release schedules van de leveranciers.</p> <p>Nieuwe versies van producten worden in overleg tussen de BsGW en de Dienstverlener geïmplementeerd.</p>	Eis		
HOST-04	De Dienstverlener realiseert en beheert de voorzieningen voor tijd- en plaatsonafhankelijk werken op de beheerde laptops van BsGW.	Eis		
HOST-05	<p>De Dienstverlener richt in samenwerking met BsGW en haar SaaS-leveranciers ketenmonitoring in voor de primaire applicaties van BsGW (Belastingapplicatie GouwIT, Waarderen applicatie Ortec, Samenwerkingsportaal ProcesFive, enz.)</p> <p>Zie ook bijlage P4 - Overzicht beveiligde verbindingen</p>	Eis		
HOST-06	In het kader van Mobile Device Management (MDM) wordt software doormiddel van een zogenaamd bedrijfsportaal naar mobile device gedistribueert.	Wens		
Back-up en uitwijk				
HOST-07	De opdrachtgever verzorgt de backup en restore van persistente data en configuraties die worden verwerkt door de platform services, waaronder SQL databases, Oracle databases, fileshares, Active Directory, virtuele machines, enz..	Eis		
HOST-08	De Dienstverlener voert periodiek (minimaal eens per kwartaal) backup en restore testen uit op alle backups waarvoor zij verantwoordelijk is. De resultaten van deze test worden gedeeld met de opdrachtgever.	Eis		
HOST-09	De dienstverlener dient back-ups op een externe locatie op te slaan waarbij maatregelen zijn genomen tegen calamiteiten.	Eis		
HOST-10	<p>De Dienstverlener voorziet in een volwaardige uitwijkomgeving die binnen de gestelde servicenormen beschikbaar is.</p> <p>Periodiek, minimaal 1 keer per jaar, wordt in overleg met de opdrachtgever de uitwijkprocedure getest. De resultaten van deze test worden gedeeld met de opdrachtgever.</p>	Eis		

HOST-11	De dienstverlener heeft een uitwijkdraaiboek voorhanden waarin minimaal is opgenomen: - Contactpersoon inclusief vervanger; - Opstartprocedure; - doorlooptijd; - Uitvoerprocedure; - Testprocedure; - gereedmeldingen.	Eis		
HOST-12	De dienstverlener dient bij het testen van de uitwijk te voldoen aan de volgende eisen en actie uit te voeren: - voldoen aan de afgesproken servicelevels en frequentie ten aanzien voor hersteltijd - technische inregeling van uitwijk bij voorbereiding uitwijk; - Testsessie uitvoeren; - Uitwijkdraaiboek beheren; - Evaluatie rapport opstellen van testsessie.	Eis		
HOST-13	De Opdrachtgever is gerechtigd bij een calamiteit naar eigen oordeel de uitwijkprocedure in werking te stellen.	Wens		
HOST-14	Het uitwijkdraaiboek is bij aanvang contract beschikbaar te zijn en zal jaarlijk worden gereviewed.	Wens		
Licenties				
HOST-15	De Dienstverlener biedt de mogelijkheid om alle benodigde licenties (incl. Microsoft) te hosten. Indien de Opdrachtgever echter wenst om bepaalde licenties elders te beleggen/aan te schaffen dient dit mogelijk te zijn.	Eis		

Tabblad 3 - Eisen en wensen Informatiebeveiliging

Aanbesteding Hosting Belastingsamenwerking Gemeenten en Waterschappen Limb

Bijlage D1 Informatiebeveiliging



nr	Omschrijving eisen	Type eis	Voldoet de aangeboden oplossing?	Toelichting
Beveiliging algemeen				
INFB-01	Informatiebeveiligingseisen worden onderdeel van het contract.	Eis		
INFB-02	Informatiebeveiligingseisen worden periodiek geëvalueerd en in samenspraak geactualiseerd.	Eis		
INFB-03	Een exit strategie is onderdeel van het contract. In deze strategie zijn bepalingen over de exit opgenomen en de condities die aanleiding zijn voor een exit.	Eis		
INFB-04	Dienstverlener adviseert Opdrachtgever over marktontwikkeling en (de leeftijd van) applicaties en technische softwarestack, strategische ontwikkelingen en innovatie voor het onderhouden van de geleverde dienst.	Eis		
INFB-05	Een toegangsbeveiligingsbeleid behoort te worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfseisen en informatiebeveiligingseisen.	Eis		
INFB-06	Een gespecialiseerde beveiligingsfunctie dient te zijn vastgesteld die verantwoordelijk is voor het bevorderen van informatiebeveiliging binnen de gehele organisatie van Dienstverlener.	Eis		

INFB-07	Dienstverlener moet een beveiligingsorganisatie gedefinieerd hebben waarin de organisatorische positie, de taken, verantwoordelijkheden en bevoegdheden (TVB) van de betrokken functionarissen en de rapportagelijnen zijn vastgesteld.	Eis		
INFB-08	Alle relevante wettelijke, statutaire, regelgevende, contractuele eisen en de aanpak van Dienstverlener om aan deze eisen te voldoen behoren voor elke clouddienst en de organisatie expliciet te worden vastgesteld, gedocumenteerd en actueel gehouden.	Eis		
INFB-09	Dienstverlener behoort een cloud-beveiligingsstrategie te hebben ontwikkeld die samenhangt met de strategische doelstelling van Dienstverlener en die aantoonbaar de informatieveiligheid ondersteunt.	Eis		
INFB-10	In de overeenkomst tussen Dienstverlener en Opdrachtgever behoort een exit strategie te zijn opgenomen waarbij zowel een aantal bepalingen over exit zijn opgenomen, als een aantal condities die aanleiding kunnen geven tot een exit.	Eis		
INFB-11	Dienstverlener past aantoonbaar relevante, nationale standaarden en internationale standaarden toe voor de opzet en exploitatie van de diensten en de interactie met Opdrachtgever. Denk aan NIST, ISO, NEN, etc.	Eis		

INFB-12	<p>Dienstverlener heeft een beheersorganisatie ingericht waarin de processtructuur en de taken, verantwoordelijkheden en bevoegdheden van de betrokken functionarissen zijn vastgesteld.</p> <p>Liefst wordt hier gebruik gemaakt van standaarden zoals ITIL.</p>	Eis		
Cryptografie				
INFB-13	Dienstverlener heeft een beleid voor het toepassen van cryptografische maatregelen voor de opslag en transport van informatie. Dit beleid is aantoonbaar geïmplementeerd in het geleverde systeem	Eis		
INFB-14	<p>Het softwarepakket past versleuteling toe op de communicatie van gegevens die passend bij het classificatieniveau is van de gegevens en controleert hierop. Het is aan Opdrachtgever om het classificatieniveau te bepalen.</p> <p>Voor de toegepaste versleutelingstechnieken worden minimaal de voor de overheid verplichte standaarden van het Forum Standaardisatie gehanteerd. Zie voor meer informatie: https://www.forumstandaardisatie.nl/open-standaarden/verplicht</p>	Eis		

INFB-15	<p>Gevoelige data van Opdrachtgever behoort conform het overeengekomen beleid inzake cryptografische maatregelen tijdens transport via netwerken en bij opslag bij Dienstverlener te zijn versleuteld.</p> <p>Voor de toegepaste versleutelingstechnieken worden minimaal de voor de overheid verplichte standaarden van het Forum Standaardisatie gehanteerd. Zie voor meer informatie: https://www.forumstandaardisatie.nl/open-standaarden/verplicht</p>	Eis		
Bedrijfscontinuïteit				
INFB-16	IT-functionaliteiten behoren te worden verleend vanuit een robuuste en beveiligde systeemketen van Dienstverlener naar Opdrachtgever.	Eis		
INFB-17	Dienstverlener behoort diens BCM-proces adequaat te hebben georganiseerd, waarbij de volgende aspecten zijn geadresseerd: verantwoordelijkheid voor BCM, beleid en procedures, bedrijfscontinuïteitsplanning, verificatie en updaten en computercentra.	Eis		
INFB-18	Dienstverlener heeft een actuele architectuur vastgelegd die voorziet in een raamwerk voor de onderlinge samenhang en afhankelijkheden van de IT-functionaliteiten.	Eis		
INFB-19	Dienstverlener behoort een risico-assessment uit te voeren, bestaande uit een risicoanalyse en risico-evaluatie met de criteria en de doelstelling voor clouddiensten van Dienstverlener.	Eis		

INFB-20	<p>Dienstverlener garandeert een maximale downtime van 16 uur (2 werkdagen) in alle voorkomende gevallen (RTO = 16 uur).</p> <p>Dit betreft de maximaal acceptabele downtime in geval van een calamiteit.</p>	Eis		
INFB-21	<p>Dienstverlener garandeert een maximaal data verlies van 8 uur (1 werkdag) in alle voorkomende gevallen (RPO = 8 uur).</p> <p>Dit betreft het maximaal acceptabele data verlies in geval van een calamiteit.</p>	Eis		
INFB-22	<p>De herstelfunctie van de data en clouddiensten, gericht op ondersteuning van bedrijfsprocessen, behoort te worden gefaciliteerd met infrastructuur en IT-diensten, die robuust zijn en periodiek worden getest.</p> <p>Dienstverlener moet bereid zijn mee te werken aan een ketentest.</p> <p>De test moet minimaal jaarlijks plaatsvinden. Van de test moet een verslag worden gemaakt.</p>	Eis		
INFB-23	<p>Risicomanagement en het risico-assessmentproces behoren continu te worden gemonitord en gereviewd en zo nodig te worden verbeterd.</p>	Eis		
Authenticatie, autorisatie, toegang en sessiebeheer				
INFB-24	<p>Sessies behoren authentiek te zijn voor elke gebruiker en behoren ongeldig gemaakt te worden na een time-out of perioden van inactiviteit. De lengte van deze time-out is door Opdrachtgever te bepalen en naderhand aan te passen.</p>	Eis		

INFB-25	De identiteit van gebruikers hoort vastgesteld te worden middels een mechanisme voor identificatie en authenticatie. Multifactorauthenticatie is hierbij altijd een optie, zonder meerkosten.	Eis		
INFB-26	Het softwarepakket behoort een autorisatiemechanisme te bieden.	Eis		
INFB-27	Het eigenaarschap en de verantwoordelijkheden voor logische toegangsbeveiligingssystemen en de verantwoordelijkheden voor fysieke toegangsbeveiligingssystemen zijn aantoonbaar vastgelegd.	Eis		
INFB-28	<p>Ter bescherming van authenticatie-informatie behoort een beleid voor het gebruik van cryptografische beheersmaatregelen te worden ontwikkeld en geïmplementeerd .</p> <p>Het hier geëiste beleid kan onderdeel zijn van het beleid dat geëist wordt in INFB.13. Als dat zo is, graag dit aangeven in de documentatie.</p>	Eis		
INFB-29	Dienstverlener behoort op basis van de organisatorische eisen en wensen de technische inrichting beschreven te hebben en behoort in een toegangsbeveiligingsarchitectuur te zijn vastgelegd.	Eis		
INFB-30	Een formele registratie- en afmeldprocedure behoort te worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken.	Eis		

INFB-31	Een formele gebruikerstoegangsverleningsprocedure behoort te worden geïmplementeerd om toegangsrechten voor alle type gebruikers en voor alle systemen en diensten toe te wijzen of in te trekken.	Eis		
INFB-32	Een formeel autorisatieproces dient geïmplementeerd te zijn voor het beheersen van de toegangsrechten van alle medewerkers en externe gebruikers tot informatie en informatie verwerkende faciliteiten.	Eis		
INFB-33	Indien het beleid voor toegangsbeveiliging (van Opdrachtgever) dit vereist, behoort toegang tot systemen en toepassingen te worden beheerst door een beveiligde inlogprocedure. Denk hierbij bijvoorbeeld (maar niet uitsluitend) aan multifactorauthenticatie voor beheerders en/of inloggen enkel vanaf bepaalde netwerken/locaties. De eisen worden door Opdrachtgever nader uitgewerkt.	Eis		
INFB-34	Systemen voor wachtwoordbeheer behoren interactief te zijn en sterke wachtwoorden te waarborgen. Het is aan Opdrachtgever om uit werken aan welke voorwaarden sterke wachtwoorden moeten voldoen.	Eis		
INFB-35	Het toewijzen en gebruik van speciale toegangsrechten behoren te worden beperkt en beheerst. Denk hierbij aan applicatie- of functioneel beheerders maar ook eventuele Dienstverleners.	Eis		

INFB-36	Conflicterende taken en verantwoordelijkheden behoren te worden gescheiden om de kans op onbevoegd of onbedoeld wijzigingen of misbruik van de bedrijfsmiddelen van de organisatie te verminderen.	Eis		
INFB-37	Het toewijzen van geheime authenticatie-informatie behoort te worden beheerst via een formeel beheersproces. Informatie zoals gebruikersnamen en wachtwoorden horen volgens een vastgestelde procedure verstrekt te	Eis		
INFB-38	Toegang (autorisatie) tot informatie en systeemfuncties van toepassingen behoren te worden beperkt in overeenstemming met het toegangsbeveiligingsbeleid. Het is aan Opdrachtgever om te bepalen wie gebruik mag maken van bepaalde functies en wie toegang mag hebben tot informatie.	Eis		
INFB-39	Ter ondersteuning van autorisatiebeheer moeten binnen de daartoe in aanmerking komende applicaties technische autorisatievoorzieningen, zoals: een personeelsregistratiesysteem, een autorisatiebeheersysteem en autorisatiefaciliteiten, beschikbaar zijn. Er moet eenvoudig en compleet inzichtelijk te maken zijn wie welke autorisaties heeft binnen het informatiebeheer.	Eis		
INFB-40	Beveiligde gebieden behoren te worden beschermd door passende toegangsbeveiliging om ervoor te zorgen dat alleen bevoegd personeel toegang krijgt.	Eis		

INFB-41	Om het gebruik van toegangsbeveiligingsvoorzieningen te (kunnen) controleren, behoren er procedures te zijn vastgesteld.	Eis		
INFB-42	Gebruikers behoren alleen toegang te krijgen tot de IT-diensten, applicatiefuncties en data waarvoor zij specifiek bevoegd zijn.	Eis		
Logging en monitoring				
INFB-43	Activiteiten van systeembeheerders en -operators behoren te worden vastgelegd en de logbestanden behoren te worden beschermd en regelmatig te worden beoordeeld.	Eis		
INFB-44	Log-bestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld. Opdrachtgever wil hier op kunnen controleren, bijvoorbeeld middels een periodieke audit.	Eis		
INFB-45	De Dienstverlener staat open voor aansluiting op SOC-	Wens		
Data en data protectie				
INFB-46	Te beschermen gegevens worden veilig opgeslagen in databases of bestanden, waarbij zeer gevoelige gegevens worden versleuteld. Opslag vindt alleen plaats als noodzakelijk. Het is aan Opdrachtgever om aan te geven welke gegevens in de categorie "zeer gevoelig" vallen.	Eis		
INFB-47	Softwarepakketten behoren mechanismen te bieden om niet-vertrouwde bestandsgegevens uit niet-vertrouwde omgevingen veilig te importeren en veilig op te slaan.	Eis		

INFB-48	Dienstverlener behoort, ter bescherming van bedrijfs- en persoonlijke data, beveiligingsmaatregelen te hebben getroffen vanuit verschillende dimensies: beveiligingsaspecten en stadia, toegang en privacy, classificatie/labels, eigenaarschap en locatie.	Eis		
INFB-49	<p>Data ('op transport', 'in verwerking' en 'in rust') met de classificatie BBN2 of hoger behoort te worden beschermd met cryptografische maatregelen en te voldoen aan Nederlandse wetgeving.</p> <p>Voor de toegepaste versleutelingstechnieken worden minimaal de voor de overheid verplichte standaarden van het Forum Standaardisatie gehanteerd. Zie voor meer informatie: https://www.forumstandaardisatie.nl/open-standaarden/verplicht</p> <p>Het is aan Opdrachtgever om data te classificeren.</p>	Eis		
INFB-50	<p>Gearchiveerde data behoort gedurende de overeengekomen bewaartermijn, technologie-onafhankelijk, raadpleegbaar, onveranderbaar en integer te worden opgeslagen en op aanwijzing van Opdrachtgever/data-eigenaar te kunnen worden vernietigd.</p> <p>Het is aan Opdrachtgever om bewaartermijnen vast te stellen.</p>	Eis		
INFB-51	Opdrachtgever gegevens behoren tijdens transport, bewerking en opslag duurzaam geïsoleerd te zijn van beheerfuncties en data van en andere dienstverlening aan andere klanten, die Dienstverlener in beheer heeft.	Eis		
INFB-52	De infrastructuur is zodanig ingericht dat de dienstverlening aan gebruikers van informatiediensten	Eis		

INFB-53	Ter bescherming tegen malware behoren beheersmaatregelen te worden geïmplementeerd voor detectie, preventie en herstel in combinatie met een passend bewustzijn van de gebruikers.	Eis		
INFB-54	De onderlinge netwerkconnecties (koppelvlakken) in de keten van Opdrachtgever naar Dienstverlener behoren te worden bewaakt en beheerst om de risico's van datalekken te beperken. Dienstverlener toont aan welke maatregelen er genomen zijn om koppelvlakken te beveiligen.	Eis		
INFB-55	De diensten van Dienstverlener zijn bruikbaar (interoperabiliteit) op verschillende IT platforms en kunnen met standaarden verschillende IT-platforms met elkaar verbinden en data overdragen (portabiliteit) naar andere Dienstverleners/cloud service providers. Voor de toegepaste versleutelingstechnieken worden minimaal de voor de overheid verplichte standaarden van het Forum Standaardisatie gehanteerd. Zie voor meer informatie: https://www.forumstandaardisatie.nl/open-standaarden/verplicht Het is aan Opdrachtgever om data te classificeren.	Eis		
INFB-56	Bij multi-tenancy wordt de klantdata binnen de infrastructuur, die door meerdere klanten worden afgenomen, in rust versleuteld en gescheiden verwerkt op gehardende (virtuele) machines.	Eis		
Toezicht				

INFB-57	Opdrachtgever behoudt zich het recht voor om audits uit te voeren/uit te laten voeren op naleving van het pakket van eisen. Dienstverlener zal hieraan (naar redelijkheid) meewerken.	Eis		
INFB-58	Dienstverlener behoort regelmatig de naleving van de beveiligingsovereenkomsten op compliance te beoordelen, jaarlijks een assurance-verklaring aan Opdrachtgever uit te brengen en te zorgen voor onderlinge aansluiting van de resultaten uit deze twee exercities.	Eis		
INFB-59	De performance van de informatiebeveiliging van de infrastructuur behoort regelmatig te worden gemonitord en hierover behoort tijdig te worden gerapporteerd aan de verschillende stakeholders, zoals Opdrachtgever.	Eis		
	Documentatie			
INFB-60	Dienstverlener behoort processen, procedures en beheersmaatregelen te documenteren, te implementeren en te handhaven. Deze zijn door Opdrachtgever op te vragen.	Eis		
INFB-61	Dienstverlener behoort haar informatiebeveiligingsbeleid uit te breiden met een cloud-beveiligingsbeleid om de voorzieningen en het gebruik van cloudservices te adresseren.	Eis		
INFB-62	Dienstverlener voorziet Opdrachtgever in een systeembeschrijving waarin de clouddiensten inzichtelijk en transparant worden gespecificeerd en waarin de jurisdictie, onderzoeksmogelijkheden en certificaten worden geadresseerd.	Eis		

INFB-63	Dienstverlener behoort de organisatie en verantwoordelijkheden voor het risicomanagementproces voor de beveiliging van clouddiensten te hebben opgezet en onderhouden.	Eis		
INFB-64	<p>Dienstverlener levert een architectuur tekening en specificeert de samenhang en beveiliging van de services en de interconnectie tussen Opdrachtgever en Dienstverlener en biedt transparantie en overzicht van randvoorwaardelijke omgevingsparameters, voor zowel de opzet, de levering en de portabiliteit van Opdrachtgever-data.</p> <p>Deze tekening wordt gedurende de contractperiode geactualiseerd door Dienstverlener op het moment dat changes of updates van invloed zijn op de beveiliging, datastromen of werking van de dienst.</p>	Eis		
INFB-65	Dienstverlener heeft een servicemanagementbeleid geformuleerd met daarin richtlijnen voor de beheersingsprocessen, controleactiviteiten en rapportages.	Eis		
Serverplatform				
INFB-66	Voor het beveiligd inrichten en onderhouden van het serverplatform behoren regels te worden vastgesteld en binnen de organisatie te worden toegepast.	Eis		
INFB-64	Principes voor het inrichten van beveiligde servers behoren te worden vastgesteld, gedocumenteerd, onderhouden en toegepast voor alle verrichtingen betreffende het inrichten van servers.	Eis		

INFB-65	Patchmanagement is procesmatig en procedureel opgezet en wordt ondersteund door richtlijnen zodat het zodanig kan worden uitgevoerd dat op de servers de laatste (beveiligings)patches tijdig zijn geïnstalleerd.	Eis		
INFB-66	Patches die als kritiek worden aangemerkt in externe bibliotheken, worden zo snel mogelijk maar uiterlijk binnen 7 dagen geïnstalleerd.	Eis		
INFB-67	Informatie over technische kwetsbaarheden van gebruikte informatiesystemen behoort tijdig te worden verkregen; de blootstelling aan dergelijke kwetsbaarheden dienen te worden geëvalueerd en passende maatregelen dienen te worden genomen om het risico dat ermee samenhangt aan te pakken.	Eis		
INFB-68	Richtlijnen en ondersteunende beveiligingsmaatregelen behoren te worden geïmplementeerd ter beveiliging van beheer op afstand van servers.	Eis		
INFB-69	Servers behoren correct te worden onderhouden om de continue beschikbaarheid en integriteit te waarborgen.	Eis		
INFB-70	Alle onderdelen van servers die opslagmedia bevatten, behoren te worden geverifieerd om te waarborgen dat gevoelige gegevens en in licentie gegeven software voorafgaand aan verwijdering of hergebruik zijn verwijderd of betrouwbaar veilig zijn overschreven.	Eis		
INFB-71	Voor het beveiligen van een server worden overbodige functies en ongeoorloofde toegang uitgeschakeld.	Eis		

INFB-72	Voor het door gebruikers (beheerders) installeren van software behoren regels te worden vastgesteld en te worden geïmplementeerd.	Eis		
INFB-73	Technische serveromgevingen behoren regelmatig te worden beoordeeld op naleving van de beleidsregels en normen van de organisatie voor servers en besturingssystemen.	Eis		
Privacy-supplement Algemeen				
INFB-74	Dienstverlener heeft privacybeleid en procedures ontwikkeld en vastgesteld, waarin de verantwoordelijkheid is vastgelegd op welke wijze persoonsgegevens worden verwerkt, invulling wordt gegeven aan de wettelijke beginselen en hoe in een cyclisch proces wordt vastgelegd op welke wijze transparant aan de wet- en regelgeving wordt voldaan en afwijkingen worden opgelost.	Eis		
INFB-75	De verdeling van de taken en verantwoordelijkheden, de benodigde middelen en de rapportagelijnen, zijn door Dienstverlener vastgelegd en vastgesteld , inclusief die bij uitwisseling van persoonsgegevens tussen Dienstverleners, zodat ook bij doorgifte van persoonsgegevens de privacybelangen van de betrokkenen, waarvan de persoonsgegevens worden verwerkt, zijn gewaarborgd.	Eis		
INFB-76	Dienstverlener waarborgt dat eenieder die persoonsgegevens verwerkt of een verwerking voorbereid zich bewust is van de belangen van de betrokkenen, waarvan de persoonsgegevens worden verwerkt, en beschouwen dit conform de verwachtingen als hoogste prioriteit om deze overtuiging toe te passen; deze betrokkenen hebben daarvoor de benodigde kennis en zijn op de hoogte van grote veranderingen in de verwachtingen.	Eis		

INFB-77	Dienstverlener heeft van eenieder, die persoonsgegevens verwerkt of een verwerking voorbereid, een actuele VOG, een actuele verklaring omtrent het naleven en de kennisname van de regels omtrent privacy en het bewijs van op de hoogte zijn van de disciplinaire procedure; hiervan bestaat een overzicht.	Eis		
INFB-78	Vooraf aan het ontwerp van een gegevensverwerking en bij een verandering wordt een inschatting gemaakt van de privacyrisico's en wordt bepaald welke passende maatregelen nodig zijn; hiervoor zijn de verantwoordelijkheden duidelijk en is er een proces ingeregeld voor het kunnen aantonen van het passend zijn van deze maatregelen.	Eis		
INFB-79	De verwerkingsverantwoordelijke(n) en de verwerker(s) hebben hun gegevens over de gegevensverwerkingen in een register vastgelegd, daarbij biedt het register een actueel en samenhangend beeld van de gegevensverwerkingen, processen en technische systemen die betrokken zijn bij het verzamelen, verwerken en doorgeven van persoonsgegevens en dat voldoet aan de vereisten van de AVG.	Eis		
INFB-80	Dienstverlener heeft de kennis georganiseerd om de oorzaak van een datalek te kunnen vaststellen en te onderzoeken, heeft daarvoor de benodigde loggegevens om herhaling te voorkomen en heeft de stakeholders vastgesteld om ze te kunnen informeren.	Eis		
Privacy-supplement SSD				
INFB-81	De oplossing voorziet er in dat standaard zo min mogelijk persoonsgegevens worden verwerkt. Standaard staan alle beschikbare technische beschermingsmaatregelen 'aan' zoals voortvloeiend uit artikel 25 AVG.	Eis		

INFB-82	Het verlenen van toegang tot persoonsgegevens wordt beperkt op basis van duidelijke en afgebakende taken en het doel en de verstrekte toegang is toetsbaar.	Eis		
INFB-83	De oplossing behoort op verwerkers/persoonsniveau te loggen, zodat direct of periodiek kan worden beoordeeld welke persoonsgegevens deze medewerker heeft opgevraagd, ingezien en aangepast.	Eis		
INFB-84	Dienstverlener behoort een proces te hebben ingericht, waarbinnen een analyse wordt gemaakt en aantoonbaar is dat het verzamelen van de persoonsgegevens rechtmatig en noodzakelijk is en het ontwerp getoetst wordt aan het uitgangspunt dataminimalisatie, de juiste wijze van opslag en het hanteren van de bewaartermijn.	Eis		
INFB-85	De oplossing behoort, indien de functionele eisen aan de oplossing van de opdrachtgever dit toelaten, gegeneraliseerde gegevens te gebruiken.	Eis		
INFB-86	Iedere oplossing kent een duidelijk verwerkingsdoel, waarbij de scheiding van de verwerking gerealiseerd is op het niveau van de oplossing, de transportpaden, de middleware, de opslagvoorzieningen en is hierop getoetst.	Eis		
Privacy-supplement Toegangsbeveiliging				
INFB-87	Dienstverlener behoort verwerkers gescheiden en beperkt toegang te verlenen tot persoonsgegevens, op basis van uit te voeren activiteiten die binnen een specifieke rol worden uitgevoerd en in te trekken, indien de activiteiten, noodzaak of vastgestelde doelbinding niet meer geldt voor deze persoon of rol; de verstrekte toegang is toetsbaar.	Eis		

INFB-88	Het verlenen van toegang tot persoonsgegevens wordt beperkt op basis van duidelijke en afgebakende taken en het doel en de verstrekte toegang is toetsbaar.	Eis		
INFB-89	De verwerking behoort op verwerkers/persoonsniveau te loggen, zodat direct of periodiek kan worden beoordeeld welke persoonsgegevens de medewerker heeft opgevraagd, ingezien en aangepast.	Eis		
INFB-90	Dienstverlener behoort fysieke beveiliging van omgevingen waar persoonsgegevens worden verwerkt, op passende wijze ingericht te hebben, zodat enkel medewerkers met noodzakelijk belang toegang hebben tot en zich bevinden in deze omgevingen; de toegang wordt geregistreerd.	Eis		
INFB-91	Er is een procedure ingericht voor het transporteren van persoonsgegevens buiten een beschermde omgeving, waarbij door versleuteling de kans op een datalek is verkleind en door minimalisatie de omvang van een datalek wordt beperkt.	Eis		
INFB-92	Dienstverlener hanteert regels voor medewerkers en andere verwerkers, die buiten Nederland persoonsgegevens of authenticatiemiddelen (voor de toegang tot persoonsgegevens vanuit het buitenland) met zich meedragen of in hun bezit hebben, ongeacht of deze informatie versleuteld is.	Eis		

INFB-93	Wanneer bedrijfsonderdelen onderhevig zijn aan wet- en regelgeving uit landen buiten de EER c.q. landen waarover de Europese Commissie geen positief adequaatheidsbesluit heeft genomen, heeft Dienstverlener daarvoor een risicoanalyse uitgevoerd t.a.v. de risico's voor de rechten en vrijheden van betrokkenen waarvan gegevens worden verwerkt in de voorziening en neemt Dienstverlener in overleg met de opdrachtgever passende maatregelen getroffen om deze risico's te mitigeren.	Eis		
INFB-94	De verwerkingsverantwoordelijke legt in de (verwerkers) overeenkomst afspraken vast, met de persoon of partij die persoonsgegevens verwerkt, over het verwijderen of overdragen van persoonsgegevens bij beëindiging van de relatie; eventuele derden worden over de beëindiging geïnformeerd.	Eis		
Privacy-supplement oplossingontwikkeling Algemeen				
INFB-95	Waar mogelijk wordt als testdata gebruik gemaakt van kunstmatig gegenereerde persoonsgegevens of fictieve data, wanneer op basis van de resultaten van een risico-analyse gebruik gemaakt wordt van persoonsgegevens, worden passende maatregelen ter bescherming van de persoonsgegevens genomen.	Eis		
Privacy-supplement Serverplatform				
INFB-96	Dienstverlener behoort een proces te hebben ingericht en afspraken te hanteren, zodat bij de configuratie van (onderdelen van) serverplatforms de instellingen gebruiken, waarbij enkel de minimaal benodigde hoeveelheid persoonsgegevens wordt verwerkt en verwijdering van persoonsgegevens mogelijk is.	Eis		

INFB-97	Dienstverlener heeft een proces ingericht, zodat bij de configuratie van (onderdelen van) serverplatforms de instellingen gebruikt worden, waarbij de scheiding van verwerkingen het uitgangspunt is.	Eis		
Privacy-supplement Communicatievoorzieningen				
INFB-98	De logging en monitoring van het netwerk behoort op verwerkers/persoonsniveau te loggen, zodat direct of periodiek kan worden beoordeeld welke persoonsgegevens deze medewerker heeft opgevraagd, ingezien en aangepast.	Eis		
Privacy-supplement Huisvesting-IV				
INFB-99	Dienstverlener heeft maatregelen getroffen die voorkomen dat de uitval van een dienst, of dit nu een eigen dienst is of van een derde is, leidt tot een datalek of andere gevolgen voor betrokkenen, waarvan de persoonsgegevens worden verwerkt, en heeft een procedure om de werking van de maatregel te evalueren.	Eis		
Privacy by Design				
INFB-100	Dienstverlener toont aan dat Privacy-by-design conform artikel 25 AVG is toepast bij de ontwikkeling van de voorziening.	Eis		
INFB-101	Dienstverlener toont aan dat Privacy-by-design conform artikel 25 AVG wordt toepast bij de doorontwikkeling van de voorziening.	Eis		