

Nr. E5	Eisen - Beveiliging en privacy	Nadere toelichting	Eis/Wens	Toelichtende omschrijving hoe uw oplossing de wens of eis realiseert. Gebruik hiervoor max. 200 woorden of anders indien aangegeven.
E5-1	Opdrachtnemer houdt zich aan de naleving van alle wetgeving (Nederlandse en Europese) aangaande privacybescherming m.b.t. de door hem geleverde oplossing en diensten.		Eis	Nvt
E5-2	Opdrachtnemer werkt volgens de normen die worden gesteld in de Baseline Informatiebeveiliging Overheid (BIO) v.w.b. de informatiebeveiliging en ISO 20000 t.b.v. service management.		Eis	Nvt
E5-3	De opslag van data vindt plaats binnen de Europese Economische Ruimte (EER), in een datacenter dat voldoet aan de Europese norm (EN 50600) of vergelijkbaar. Hiervoor wordt een volledige leveringsketenbeschrijving geëist.	Aangeven locaties datacenters door Opdrachtnemer (bij inschrijving)	Eis	Nvt
E5-4	De infrastructuur en organisatie van de opdrachtnemer zijn adequaat beveiligd volgens ISO/IEC 27001 en ISO/IEC 27002 of vergelijkbaar. Opdrachtnemer is bereid op verzoek een verklaring van getrouwheid (of vergelijkbaar) te verkrijgen via een onafhankelijke derde partij (TPM).		Eis	Nvt
E5-5	De infrastructuur en organisatie van de opdrachtnemer zijn adequaat beveiligd volgens de geldende DigiD-normen. Opdrachtnemer overlegt hiertoe jaarlijks, uiterlijk op 30 september, een verklaring van getrouwheid (of vergelijkbaar) te verkrijgen via een onafhankelijke derde partij (TPM).		Eis	Nvt
E5-6	Tussen de opdrachtgever en opdrachtnemer wordt een verwerkersovereenkomst afgesloten op basis van het VNG/IBD formaat welke de opdrachtgever hanteert.		Eis	Nvt
E5-7	Vulnerability assessments (security scans en pentest) worden periodiek uitgevoerd (minimaal 1 x per jaar).		Eis	Nvt
E5-8	Rapportages omtrent de veiligheid van de oplossing worden gedeeld met de opdrachtgever.		Eis	Nvt
E5-9	De aangeboden oplossing legt een audit-trail vast over het gebruik van het systeem. Deze audit-trail bevat alle handelingen m.b.t. gebruikersautorisaties en functioneel gebruik (van medewerkers opdrachtgever) van het systeemzoals raadplegen, aanmaken, muteren, verwijderen van informatie. Vastlegging vindt minimaal plaats op gebruikersniveau en -rol, tijdstip en verrichte actie en is inzichtelijk voor zowel de functioneel beheerder, de functionaris gegevensbescherming, CISO en Privacy Officer van de opdrachtgever.	Dit moet zowel voldoen aan hoofdstuk 2.1.23 van het Logisch Ontwerp BRP (versie 4.2.0) én aan de eisen die de BIO beschrijft m.b.t. logging (ook verwerkt in GIBIT-voorwaarden). Daarnaast moet dit een basis kunnen bieden om rechten van betrokkene te kunnen waarborgen (=AVG) en indien mogelijk/van toepassing een basis bieden voor toekomstige verplichtingen o.g.v. regie op eigen gegevens.	Eis	Beschrijf in maximaal 1 A4 hoe uw oplossing hierin voorziet.
E5-10	Opdrachtnemer garandeert dat ongeautoriseerde personen geen toegang hebben tot gegevens of gegevensdragers (zoals harde schijven en back-upmedia) die tussentijds of na beëindiging van de overeenkomst worden verwijderd c.q. worden vervangen.		Eis	Nvt
E5-11	Opdrachtnemer zal indien hij (pogingen tot) ongeautoriseerde toegang tot de systeemomgeving signaleert, alle noodzakelijke maatregelen nemen teneinde de eventuele schade tot een minimum te beperken en herhaling te voorkomen. De (poging tot) ongeautoriseerde toegang alsmede alle getroffen maatregelen zullen aan de opdrachtgever worden gerapporteerd.		Eis	Nvt
E5-12	Opdrachtnemer verleent medewerking aan het uitoefenen van controle door of namens opdrachtgever op bewaring en gebruik van data, en naleving van procedures;	Voortbordurend op de logging, niet alleen vastleggen ook controleren	Eis	Nvt
E5-13	Opdrachtnemer voldoet met de geboden oplossing aan de AVG en BRP mbt tot dataminimalisatie en privacyrechten.		Eis	Nvt
E5-14	De test-/acceptatieomgeving is inzetbaar met behulp van goedgekeurde testsets, bijvoorbeeld van de RvIG.	Testen mag nooit met productiedata, ook niet geanonimiseerd.	Eis	Nvt
E5-15	Opdrachtnemer kan op verzoek een autorisatiematrix aanleveren, waarin per bedrijfsfunctie is vastgelegd welke rol iemand mag hebben in de geboden oplossing	Onderdeel van jaarlijkse DigiD aansluiting audit	Eis	Nvt
E5-16a	Opslag van data van Opdrachtgever: de data die door Opdrachtgever wordt opgenomen in de door Opdrachtnemer beheerde applicatie wordt door Opdrachtnemer uitsluitend opgeslagen binnen deze applicatie en de daarbij behorende componenten, waaronder databases en back-up media.		Eis	Nvt
E5-16b	Toegang tot de data door Opdrachtnemer: Het is Opdrachtnemer toegestaan rechtstreeks toegang tot de data te verkrijgen indien dit noodzakelijk is in het kader van: i. een spoedeisend belang om de beschikbaarheid, integriteit of vertrouwelijkheid van de applicatie te waarborgen; ii. in overleg met Opdrachtgever in het kader van de afwikkeling van incidenten en ondersteuningsvragen door het support center; iii. in overleg met Opdrachtgever in het kader van de implementatie van wijzigingen aan de applicatie door het support center, consultants of developers; iiii. indien een wettelijk voorschrift Opdrachtnemer hiertoe verplicht.		Eis	Nvt
E5-16c	Logging van de toegang: i. Van de toegang tot de data legt de applicatie automatisch in het logboek van de omgeving vast welke medewerker, op welk moment is ingelogd en welke data is bekeken of gewijzigd; ii. Deze onder i genoemde logging is te allen tijde actueel en toegankelijk voor Opdrachtgever.		Eis	Beschrijf in maximaal 1 A4 hoe uw oplossing hierin voorziet.
E5-17	De geboden oplossing voorziet in goede scheiding tussen systeembeheer, functioneel- en technisch- applicatiebeheer en gebruikers		Eis	Nvt
E5-18	Er wordt een toereikend en aantoonbaar recovery proces ingericht waar back-up en restore onderdeel vanuit maken	Backup retentie : de backup dient te voldoen aan de volgende retentietijden (voorbeeld): • Elke dag met een retentie van 14 dagen; • Elke zaterdag van de week met een retentie van 4 weken; • Elke eerste dag van de maand met een retentie van 6 maanden Backup locatie: Inrichting vindt plaats volgens de “3-2-1 Methode”. Deze methode stelt dat u minimaal 3 kopieën van uw data hebt, die op 2 verschillende media staan en waarvan 1 op een andere locatie wordt opgeslagen.	Eis	Nvt
E5-19	Opdrachtnemer draagt zorg voor een toereikend back-up en restore proces mbt de geboden oplossing.	Ook wet BRP en diverse bijzondere wetten op het gebied van burgerzaken (documenten, covog) zijn van toepassing.	Eis	Nvt
E5-20	De geboden oplossing kan systeemrapportages uitdraaien over het gebruik van de applicatie (systeem logging)		Eis	Nvt
E5-21	In de overeenkomst behoort een exit strategie te zijn opgenomen waarbij zowel een aantal bepalingen aangaande exit zijn opgenomen, als een aantal condities die aanleiding kunnen geven tot een exit.		Eis	Nvt

E5-22	De Opdrachtnemer draagt bij beëindiging van het contract alle data (inclusief metadata) uit het informatiesysteem in een origineel én duurzaam bestandsformaat over aan de Opdrachtgever. Het bestand wordt zodanig aan de opdrachtgever geleverd dat de samenhang en structuur van de informatie behouden blijft. De oude leverancier werkt mee aan een transitieplan om alle metadata en documenten over te helpen brengen naar het nieuwe systeem. De ontvangen bestanden zijn eenvoudig leesbaar en kunnen zonder extra kosten worden verwerkt in bijv. een informatiesysteem (DMS cq Zaaksysteem) of e-depot. Aanvullend daarop: - De data is ten allen tijde geautomatiseerd te onttrekken richting bijv. een (Azure of ander) datawarehouse - Dit proces gaat op een veilig manier - Er zitten geen extra kosten aan		Eis	Nvt
E5-23	Alle relevante wettelijke, statutaire, regelgevende, contractuele eisen en de aanpak van de opdrachtnemer om aan de eisen te voldoen, behoren voor elke dienst en voor de opdrachtgever expliciet te worden vastgesteld, gedocumenteerd en actueel gehouden.		Eis	Nvt
E5-24	De opdrachtnemer behoort de organisatie en verantwoordelijkheden voor het risicomanagement proces voor de beveiliging van de diensten te hebben opgezet en te onderhouden.		Eis	Nvt
E5-25	Informatieverwerkende faciliteiten behoren met voldoende redundantie te worden geïmplementeerd om aan continuïteitseisen te voldoen.		Eis	Nvt
E5-26	De herstelfunctie van data en diensten, gericht op ondersteuning van bedrijfsprocessen behoort te worden gefaciliteerd met infrastructuur en IT-diensten, die robuust zijn en periodiek worden getest.		Eis	Nvt
E5-27	Inschrijver behoort een Business Continuity Management (BCM) proces adequaat te hebben georganiseerd, waar bij de volgende aspecten zijn geadresseerd: verantwoordelijkheid voor BCM, beleid en procedures, business continuity planning, verificatie en updaten, en computercentra.		Eis	Nvt
E5-28	HTTPS verkeer is encrypted op TLS 1.2 niveau of hoger		Eis	Nvt
	Privacy-by-design Systeemeisen			
E5-29	Persoonsgegevens kunnen in de Oplossing getoetst worden aan authentieke brongegevens op het moment van verwerking om te controleren op juistheid.	Een toets aan authentieke brongegevens draagt bij aan de juistheid van de persoonsgegevens. Deze toets dient zo dicht mogelijk aan de verwerking zelf te liggen en alleen wanneer noodzakelijk voor de verwerking, wat er voor zorgt dat deze toets heel tijdsgebonden en op het niveau van de individuele verwerking kan plaatsvinden.	Eis	Nvt
E5-30	De accuraatheid en kwaliteit (integriteit) van persoonsgegevens kunnen via invoermechanismes en importmechanismes afgedwongen worden. Hiervoor is een definitie-woordenboek en datamodel beschikbaar. Noodzakelijke gegevensvelden zijn indien noodzakelijk aan te passen.	De Oplossing moet het mogelijk maken dat in hoge mate controle is op de input en import van gegevens in de Oplossing, enerzijds met een beschrijving (definities, semantiek) van gegevensvelden in een gegevenswoordenboek en datamodel (hiërarchie gegevens), anderzijds door technische hulpmiddelen om juistheid van persoonsgegevens af te dwingen. Voorbeelden hiervan zijn voorgedefinieerde velden in plaats van open velden of voorzieningen om gegevens te valideren bij import.	Eis	Nvt
E5-31	Alle vormen van verwerkingen van persoonsgegevens dienen gelogd te worden in een niet-muteerbare audittrail. Hierbij dient maximaal informatie gelogd te worden die nodig is om de gebeurtenis te herleiden tot een functie of rol en minimaal het resultaat van de handeling en een datum en tijd van de gebeurtenis. De beschikbaarheid van loginformatie is gegarandeerd totdat de bewaartermijn van de persoonsgegevens verlopen is en de loginformatie dient daarna verwijderd te worden.	Het doel van loggen voor privacybescherming is anders dan loggen voor informatiebeveiliging: het achteraf kunnen aantonen dat een gegevensverwerking rechtmatig verlopen is. Loggen is zelf ook een gegevensverwerking, waardoor het loggen zelf ook naast alle privacy by design-eisen gelegd dient te worden. Loginformatie dient bijvoorbeeld beveiligd te zijn, minimaal en liefst gedistribueerd opgezet te zijn.	Eis	Beschrijf in maximaal 1 A4 hoe uw oplossing hierin voorziet.
E5-32	Bij de Oplossing wordt documentatie geleverd die alle door de leverancier genomen privacymaatregelen op een voor betrokkenen heldere manier beschrijft. Deze documentatie kan ook opgeleverd worden als onderdeel van de verwerkersovereenkomst.	Documentatie op het niveau van de Oplossing over privacybeschermende maatregelen dienen in het register opgenomen te kunnen worden, zodat deze gebruikt kan worden om verwerkende medewerkers, toezichhoudende instanties en betrokkenen te informeren. Hieronder vallen ook eventuele certificeringen en controlerapporten over privacybeschermende maatregelen.	Eis	Nvt

Nr. W5	Wensen - Beveiliging en Privacy	Toelichting	Wens	Toelichtende omschrijving hoe uw oplossing de wens of eis realiseert. Gebruik hiervoor max. 200 woorden of anders indien aangegeven.	Aantal punten
--------	---------------------------------	-------------	------	--	---------------

Geen wensen tav onderwerp Beveiliging en Privacy