Bijlage 2b
Programma van Eisen / Non Functioneel

Nr.	ID	Domein	Stelling (NL)	Toelichting (NL)
1	PS-001	Privacy & Security	Communicatie van systeem gebeurt met HAN huisstijl	De gebruiker moet eventuele door het systeem verstuurde berichten kunnen herkennen als zijnde een door het systeem en namens de HAN verstuurd bericht. Het afzender e-mailadres moet eindigen op “han.nl” (of een subdomein van “han.nl”) door gebruik te maken van SPF/DKIM welke geregistreerd worden in de DNS van de HAN (HAN).
2	PS-002	Privacy & Security	Privacy & Security	Privacy by default en Privacy by design zijn toegepast. Nadere omschrijving hoe dit is toegepast (pas toe of leg uit) kan door de opdrachtnemer worden overlegd. Bijvoorbeeld : Pas toe: Ons systeem implementeert privacy by design, met standaard versleuteling van gegevens en dataminimalisatie ingebouwd vanaf de ontwerpfase. OF Leg uit: Vanwege technische beperkingen passen we geen volledige dataminimalisatie toe. Echter wij compenseren dit met strengere toegangscontrole en regelmatige audits van de gegevensverwerking.
3	PS-003	Privacy & Security	Voldoet aan privacy by design	Opdrachtnemer heeft aantoonbare en duidelijke geheimhoudingsafspraken met zijn medewerkers.
4	PS-004	Privacy & Security	Voldoet aan bewaartermijnen	De door de HAN (in overleg met de archivaris) vastgestelde bewaartermijnen kunnen door de gehele keten van (sub)verwerkers worden ingeregeld en geïmplementeerd.
5	PS-005	Privacy & Security	Voldoet aan verwijderingstermijnen	In de gehele keten van de verwerking geldt dat na einde van de bewaartermijnen de data wordt verwijderd overeenkomstig de met de HAN af te spreken vernietigingstermijnen.
6	PS-006	Privacy & Security	Subverwerkers voldoen aan dezelfde beveiligings- en privacyvereisten (data) als de hoofdverwerker	Alle data (inclusief backups of kopieën) van de HAN moet te allen tijde aleen worden opgeslagen binnen de grenzen van de Europese Economische Ruimte (EER), óf in een land waar een adequaatheidsbesluit (adequacy decision) van de Europese Commissie van toepassing is. Dit geldt ook voor de subverwerkers die worden ingeschakeld door de verwerker.
7	PS-007	Privacy & Security	Subverwerkers voldoen aan dezelfde beveiligings- en privacyvereisten (afspraken) als de hoofdverwerker	De afspraken die met de opdrachtnemer worden gemaakt ten aanzien van de verwerking van persoonsgegevens, beveiliging hiervan en de geheimhoudingsverplichting van medewerkers werken 1 op 1 door voor de ingeschakelde subverwerkers. Hiervan kan documentatie worden overlegd waarin deze afspraken zijn vastgelegd.
8	PS-008	Privacy & Security	Subverwerkers voldoen aan dezelfde beveiligings- en privacyvereisten (maatregelen) als de hoofdverwerker	De opdrachtnemer kan opgaaf van doen van alle subverwerkers en locaties waar de data wordt verwerkt door de gehele keten heen inclusief de afspraken die met deze partijen zijn gemaakt. Daarnaast kan de verwerker aantonen dat alle subverwerkers passende organisatorische en technische maatregelen hebben genomen om de gegevens die in opdracht worden verwerkt, te beschermen.
9	PS-009	Privacy & Security	Subverwerkers voldoen aan dezelfde beveiligings- en privacyvereisten	Bij wijziging van een subverwerkers is vooraf toestemming van de HAN noodzakelijk.
10	PS-010	Privacy & Security	Gegevens zijn geanonimiseerd	Niet-productie omgevingen van het systeem maken gebruik van geanonimiseerde of fictieve gegevens. (Bij het anonimiseren van persoonsgegevens worden de gegevens zó veranderd dat op geen enkele wijze meer is te achterhalen is over wie de gegevens gaan.)
11	PS-011	Privacy & Security	Toegang tot persoonsgegevens is beperkt	De toegang tot persoonsgegevens is beperkt tot het noodzakelijke (Least Privilege principe).
12	PS-012	Privacy & Security	ICT-oplossing voldoet aan portabiliteit	Het systeem is zodanig ontwikkeld en ingericht dat de gegevens desgewenst kunnen worden overgedragen naar een ander informatiesysteem (‘portabiliteit’). Relevant vanwege rechten van betrokkenen.
13	PS-013	Privacy & Security	Voldoet aan wetgeving (grondslag)	Voor elke verwerking van persoonsgegevens dient een wettelijke grondslag aanwezig te zijn. Voor bijzondere, gevoelige of strafrechtelijke persoonsgegevens geldt in beginsel een verbod op de verwerking ervan.
14	PS-014	Privacy & Security	AI-toepassingen moeten ethisch verantwoord en transparant zijn om vertrouwen en veiligheid te waarborgen	De opdrachtnemer toont aan of er sprake is van (generatieve) AI toepassingen en tot welke risicoklasse(n) deze behoren. Verder toont de oprachtnemer aan te voldoen aan de eisen die worden gesteld aan aanbieder van AI-systemen en biedt geen verboden AI-toepassingen aan. Het is mogelijk deze AI toepassing uit te schakelen.
15	PS-015	Privacy & Security	Effectieve authenticatie is de sleutel tot veilige toegang tot systemen en informatie.	Naast het gebruik van systemen dient ook onderhoud en beheer op de systemen wordt met 2-factorauthenticatie uitgevoerd. De oplossing van de opdrachtnemer faciliteert dat medewerkers van de instelling inloggen via de identity provisioning (ID-P) voorziening van de instelling. De oplossing ondersteunt daarbij dat instellingen 2-factorauthenticatie gebruiken. De opdrachtnemer is verplicht om een adequaat Privileged Access Management (PAM) proces in te richten voor al hun beheer- en onderhoudsaccounts op het af te nemen applicatie- of SaaS-platform. Dit omvat alle accounts die toegang hebben tot gevoelige of kritische onderdelen van het platform voor het uitvoeren van beheertaken, onderhoudswerkzaamheden en probleemoplossing. Criteria: •Beveiligde toegang: Alle beheer- en onderhoudsaccounts moeten gebruik maken van multi-factor authenticatie (MFA) en sterke wachtwoorden conform de geldende beveiligingsnormen. •Toegang minimaliseren: Toegang tot beheeraccounts dient gebaseerd te zijn op het principe van “least privilege”, wat betekent dat gebruikers alleen toegang krijgen tot de onderdelen die noodzakelijk zijn voor de uitvoering van hun taak. •Tijdelijke toegang: Voor werkzaamheden waarbij verhoogde rechten nodig zijn, moet de toegang tijdelijk worden verleend en automatisch worden ingetrokken zodra de taak is afgerond (just-in-time toegang). •Logging en monitoring: Alle activiteiten die worden uitgevoerd door beheer- en onderhoudsaccounts moeten volledig worden gelogd en gemonitord. Deze logs moeten minimaal 12 maanden worden bewaard en periodiek worden gecontroleerd op ongeautoriseerde toegangspogingen of afwijkend gedrag. •Audits en rapportages: De opdrachtnemer moet periodiek (bijvoorbeeld halfjaarlijks) rapportages verstrekken over het gebruik van beheer- en onderhoudsaccounts, inclusief wie toegang heeft gehad, waarvoor, en de duur van de toegang. •Toegangsevaluatie: De opdrachtnemer dient minimaal één keer per kwartaal een evaluatie uit te voeren van alle beheer- en onderhoudsaccounts om te verifiëren of de verleende rechten nog steeds noodzakelijk zijn.
16	PS-017	Privacy & Security	Betrokken partijen (commercie) zijn vastgelegd	Informatie over een instelling wordt door externe opdrachtnemer niet zonder voorafgaande toestemming aan derden ter beschikking gesteld, bijvoorbeeld voor commerciële doeleinden.
17	PS-018	Privacy & Security	Betrokken partijen (training) zijn vastgelegd	De betrokken medewerkers van de Opdrachtnemer zijn aantoonbaar getraind in het veilig en het juist beheer en gebruik van het systeem.
18	PS-019	Privacy & Security	Betrokken partijen (incidenten) zijn vastgelegd	Richtlijnen en procedures voor de melding, registratie en het oplossen van incidenten (waaronder beveiligingsincidenten en datalekken) zijn schriftelijk vastgelegd.

19	PS-020	Privacy & Security	Betrokken partijen (capaciteit) zijn vastgelegd	Richtlijnen en procedures voor de bepaling van het huidige en het toekomstige gebruik van het systeem (capaciteitsplanning) zijn schriftelijk vastgelegd.
20	PS-023	Privacy & Security	Betrokken partijen (testen) zijn vastgelegd	Richtlijnen en procedures voor het beheer en de beveiliging van testgegevens zijn schriftelijk vastgelegd. Testen in een testomgeving wordt alleen gedaan met fictieve of anonieme persoonsgegevens. Indien dit niet mogelijk is, dient te worden uitgelegd waarom en dient hiervoor uitdrukkelijk toestemming te worden gevraagd.
21	PS-025	Privacy & Security	Betrokken partijen (DPIA) zijn vastgelegd	De opdrachtnemer is verplicht medewerking te verlenen als er door of namens SURF dan wel de instellingen een DPIA wordt uitgevoerd. Dit geldt ook voor een FRIA, DTIA en IB-risicoanalyse. Een DPIA is verplicht voordat nieuwe systemen of diensten bij de HAN worden geïmplementeerd die een potentieel risico vormen voor de privacy van betrokkenen. Dit helpt bij het identificeren en verminderen van de privacyrisico's.
22	PS-026	Privacy & Security	Opdrachtnemer voldoet aan beveiligingseisen (TLS)	Het systeem of webapp maakt gebruik van https en is voorzien van een TLS-certificaat (meest actuele veilige industrie standaard versie). Na de aanbestedingsfase zorgt de opdrachtnemer ervoor dat deze tijdig up-to-date blijft.
23	PS-027	Privacy & Security	Opdrachtnemer voldoet aan beveiligingseisen (verwerkersovereenkomst)	De oplossing faciliteert dat gebruikers op de juiste wijze worden geïnformeerd over de verwerking van hun persoonsgegevens in de oplossing, waaronder het loggen van de activiteiten. Comform de informatieplicht onder de AVG, artikel 13.
24	PS-028	Privacy & Security	Opdrachtnemer voldoet aan beveiligingseisen (logging)	Het systeem heeft zowel voor gebruikers als beheerders (instelbare) middelen voor de logging van activiteiten (raadplegen van gegevens, invoeren van gegevens, opslaan van gegevens, verwerken van gegevens, verzenden en ontvangen van berichten, geven of intrekken van autorisatie, etc.).
25	PS-029	Privacy & Security	Opdrachtnemer voldoet aan beveiligingseisen (veilig programmeren)	Het systeem is ontwikkeld met gebruik van veilig programmeren (zie bijvoorbeeld https://www.ncsc.nl/ en https://www.owasp.org/).
26	PS-030	Privacy & Security	Opdrachtnemer voldoet aan beveiligingseisen (encryptie)	Gegevens worden, wanneer ze in rust zijn (data at rest), opgeslagen met gebruik van encryptie volgens industriestandaardtechnieken, met een adequate sleutellengte en een sterk algoritme. (Encryptie Data at rest: AES-256 (zie: https://www.forumstandaardisatie.nl/open-standaarden/aes)) Voor opslag van gegevens wordt gebruikt gemaakt van een dienst zoals Cloud Storage Encryption (CSE), bijvoorbeeld van Microsoft. De diensten voor opslag maken gebruik van van AES-256 encryptie, sleutellengte = 256, algoritme = Diffie-Hellman Groep 14. Voor On-presmises opslag, wordt Full Disk Encryption (FDE) technieken toegepast, zoals Microsoft BitLocker voor on-premise opslag. Gegevens worden, wanneer ze tijdens transport zijn (data in transit), versleuteld met gebruik van encryptie volgens industriestandaardtechnieken, met een adequate sleutellengte en een sterk algoritme, om veilige overdracht te waarborgen. (Encryptie Data in transit: TLS 1.3 (zie: https://www.forumstandaardisatie.nl/open-standaarden/tls))
27	PS-031	Privacy & Security	SLA overeenkomst is ondertekend	Er is een Service Level Agreement (SLA) van toepassing (voor ondertekening van het contract) waarin het niveau van de beschikbaarheid en andere belangrijke kenmeken van de oplossing is vastgelegd.
28	PS-032	Privacy & Security	Taken en verantwoordelijkheden zijn belegd	Taken en verantwoordelijkheden voor het beheer en de beveiliging van het systeem zijn gedefinieerd en schriftelijk vastgelegd, bij voorkeur met gebruik van ITIL of een vergelijkbare gestructureerde methode voor ICT-beheer. (Er is een Service Level Agreement (SLA) van toepassing (vóórafgaand aan de ondertekening van het contract) waarin het niveau van de beschikbaarheid en andere belangrijke kenmeken van de oplossing is vastgelegd.)
29	PS-033	Privacy & Security	Rapportages zijn belegd	Rapportage over de mate waarin de oplossing en aanverwante diensten voldoen aan de toepasselijke normen uit de SLA, vindt plaats volgens een vooraf vastgestelde en overeengekomen inhoud en frequentie.
30	PS-034	Privacy & Security	Verbinding is versleuteld	Personeel van de cloudprovider heeft op afstand alleen op een veilige manier toegang tot de omgeving: • via een versleutelde VPN-verbinding • met behulp van tweefactor authenticatie • met een sessie-time-out, maximaal 1 uur.
31	PS-035	Privacy & Security	Toegang is gelogd	Het verkrijgen van toegang tot het systeem worden gelogd. De logfile wordt voor analysedoeleinden bewaard.
32	PS-036	Privacy & Security	ICToplossing heeft een aantoonbaar hardeningsbeleid	De opdrachtnemer dient een aantoonbaar passend hardeningsbeleid en -proces te hebben voor alle relevante systemen waarop het systeem wordt gehost. Dit omvat onder andere het verwijderen van standaardconfiguraties en systeemwachtwoorden, evenals andere maatregelen om de systemen te beschermen tegen cyber en fysieke aanvallen.
33	PS-037	Privacy & Security	Het systeem wordt gehost op afzonderlijke hardware of in een multi-tenant omgeving	Het systeem wordt gehost op afzonderlijke hardware, of in een zodanig gedeelde infrastructuur (multi-tenant omgeving), dat de beveiliging van de omgeving van de HAN niet in gevaar kan worden gebracht. De opdrachtnemer dient aantoonbaar te garanderen dat de scheiding tussen de klanten adequaat is geïmplementeerd en dat beveiligingsrisico's die voortkomen uit de gedeelde infrastructuur worden gemitigeerd.
34	PS-038	Privacy & Security	Routers en firewalls zijn ingericht	De opdrachtnemer dient er aantoonbaar voor te zorgen dat routers en firewalls zodanig zijn ingericht dat: •Er slechts één of zeer beperkte en gecontroleerde toegang tot het systeem wordt gebruikt voor inkomend verkeer, om controle te behouden over de toegang. •De configuratie voldoet aan de best practices van de opdrachtnemer en algemeen geaccepteerde beveiligingsnormen. •Er redundantie aanwezig is, zodat meerdere beveiligingslagen voorkomen dat één enkel falen tot een kwetsbaarheid leidt. •Diverse soorten beveiligingsmaatregelen worden gebruikt om een breed scala aan potentiële bedreigingen af te dekken. •Bij het falen van een beveiligingsmechanisme er geen ongeoorloofde toegang wordt verleend. •De firewall technologie gebruik maakt van geavanceerde methoden om netwerkverkeer actief te monitoren en te controleren.
35	PS-039	Privacy & Security	kwetsbaarhedenbeleid is vastgesteld	De opdrachtnemer dient een aantoonbaar kwetsbaarhedenbeleid en proces te hebben vastgesteld in en in gebruik te hebben voor de relevante informatiesystemen en onderliggende infrastructuur met passende monitoring en logging op dit proces.
36	PS-040	Privacy & Security	Cloudprovider	In de productieomgeving is alleen uitvoerbare code aanwezig.
37	PS-041	Privacy & Security	Afvoer van apparatuur gebeurt secuur	De cloudprovider draagt er zorg voor dat afvoer van apparatuur, waarop zich gegevens van het systeem bevinden of hebben bevonden, op een veilige en gecertificeerde manier wordt uitgevoerd.
38	PS-042	Privacy & Security	Beschikbaarheid is gewaarborgd	Er zijn procedures en voorzieningen aanwezig voor de waarborging van de beschikbaarheid en de back-up van de programmatuur en de inhoudelijke gegevens, inclusief externe opslag van de back-ups.

39	PS-044	Privacy & Security	Back-ups zijn gewaarborgd	De opdrachtnemer test de geldigheid en volledigheid van de back-up jaarlijks door het uitvoeren van een restore op een andere omgeving. De frequentie van het testen van back-ups moet afgestemd zijn op de beschikbaarheidsvereisten zoals gedefinieerd in de BIV-classificatie (Beschikbaarheid, Integriteit, Vertrouwelijkheid) en de Recovery Point Objective (RPO). Als de beschikbaarheidseisen hoog zijn en de RPO kort is, zal een hogere testfrequentie vereist zijn om de continuïteit en beschikbaarheid van gegevens te waarborgen.
40	PS-045	Privacy & Security	Penetratietesten worden jaarlijks uitgevoerd	Het Systeem/Platform en de technische IT infrastructuur van opdrachtnemer moeten minimaal jaarlijks worden getest door middel van penetratietests en kwetsbaarhedenscans om potentiële beveiligingslekken vroegtijdig op te sporen en aan te pakken. Minimaal dienen de kritieke bevindingen die hieruit voortkomen opgelost te worden binnen de vooraf bepaalde oplostermijn.
41	PS-046	Privacy & Security	Recht op controle	De betrokken instellingen hebben het recht om de organisatorische en technische maatregelen te (laten) controleren.
42	PS-047	Privacy & Security	Opdrachtnemer informeert opdrachtgever bij kwetsbaarheden	De Opdrachtnemer is verplicht om de instelling te informeren als er kwetsbaarheden worden aangetroffen in gecontracteerde IT-diensten. Deze melding hoeft geen technische details te bevatten, maar bevat in ieder geval een indicatie van het risico voor de instelling vanwege de kwetsbaarheid, verwachte tijdlijnen voor het aanpakken van de kwetsbaarheid, een uitgebreid overzicht van stappen die de instelling kan nemen om het risico van de kwetsbaarheid te verkleinen en of er aanwijzingen zijn dat er misbruik is gemaakt van de kwetsbaarheid.
43	PS-048	Privacy & Security	Informatiebeveiliging is gewaarborgd	De cloudprovider heeft aantoonbaar algemeen geaccepteerde standaarden voor informatiebeveiliging geïmplementeerd (bijvoorbeeld ISO 27001). Indien de opdrachtnemer niet ISO 27001-gecertificeerd is, dient zij aan te tonen welke gelijkwaardige maatregelen of standaarden zijn toegepast om een vergelijkbaar niveau van informatiebeveiliging te waarborgen. Alle getroffen organisatorische en technische maatregelen dienen passend te zijn voor de door de HAN gestelde BIV-classificatie van de verwerkingen.
44	PS-050	Privacy & Security	Data Loss Prevention (DLP) maatregelen zijn vastgelegd	Het Systeem/Platform moet in staat zijn om mechanismen zoals monitoring en preventie te bieden voor het onbedoeld verlies van gegevens, bijvoorbeeld door het blokkeren van ongeautoriseerde overdracht van vertrouwelijke informatie via e-mail of andere kanalen.
45	PS-051	Privacy & Security	Training voor medewerkers is gewaarborgd	Alle medewerkers in uw organisatie die met gevoelige informatie werken moeten periodiek worden getraind om bewust te blijven van de laatste bedreigingen, phishing-aanvallen, en best practices voor het veilig omgaan met gegevens.
46	PS-053	Privacy & Security	Incident Response maatregelen zijn vastgelegd	Het organisatie en het platform moet in staat zijn om effectief te reageren op veiligheidsincidenten (aansluitend op de incidentmanagement procedure) door integratie met een Incident Response team, inclusief de mogelijkheid om snel te reageren op bedreigingen en escalatieprocedures voor ernstige incidenten.
47	PS-054	Privacy & Security	Verwerkersovereenkomst is afgesloten	Opdrachtgever committeert zich aan het gebruik van de model verwerkersovereenkomst zoals ter beschikking gesteld door de HAN.
48	PS-055	Privacy & Security	IP-whitelisting is vastgelegd	IP-whitelisting zorgt ervoor dat alleen specifieke, goedgekeurde IP-adressen toegang kunnen krijgen tot de systemen. Dit versterkt de beveiliging door ongeautoriseerde toegang van onbekende bronnen te blokkeren. Het systeem/platform moet IP-whitelisting ondersteunen om alleen toegang te verlenen aan goedgekeurde IP-adressen.
49	PS-056	Privacy & Security	Opdrachtnemer is gecertificeerd	De opdrachtnemer dient gecertificeerd te zijn voor industriestandaard informatiebeveiligingsnormen zoals ISO27001, ISO27017, NEN7510, en bij financiële dienstverlening ook ISAE 3402 type 2. Indien de opdrachtnemer niet gecertificeerd is, moet deze aantonen hoe wordt voldaan aan het SURFToetsingskader of ISO27001/2 via het pas toe of leg uit principe. Deze certificeringen en bijbehorende verklaring van toepasselijkheid waarborgen de implementatie van de noodzakelijke informatiebeveiligingsmaatregelen. Als een opdrachtnemer niet gecertificeerd is, dient men te kunnen aantonen hoe aan de betreffende normen wordt voldaan, bijvoorbeeld via een recht van audit van de HAN of self-assessment.
50	PS-057	Privacy & Security	Opdrachtnemer voldoet aan AVG	De opdrachtnemer dient te voldoen aan de Algemene Verordening Gegevensbescherming (AVG) en moet kunnen aantonen hoe de verordening is geïmplementeerd, inclusief de beginselen van privacy by design en default, dataminimalisatie, en het recht op toegang, correctie en verwijdering van gegevens.
51	PS-058	Privacy & Security	Opdrachtnemer voldoet aaninformatiebeveiligingsnormen	De SaaS-opdrachtnemer dient te waarborgen dat subverwerkers, zoals hosting- en storagepartners, voldoen aan passende informatiebeveiligingsmaatregelen conform ISO 27017/18. De opdrachtnemer moet kunnen aantonen dat zij "in control" zijn over de beveiligingspraktijken van hun subverwerkers. De SaaS-opdrachtnemer draagt verantwoordelijkheid voor het controleren en waarborgen van de informatiebeveiliging van hun subverwerkers. Dit omvat het uitvoeren van due diligence, het vastleggen van beveiligingsvereisten in contracten en het monitoren van de naleving van deze maatregelen door de subverwerkers.
52	PS-059	Privacy & Security	Doorgifte persoonsgegevens	Binnen de gehele keten van (sub)verwerkingen worden er geen persoonsgegevens doorgegeven buiten de EER, tenzij er sprake is van aantoonbare passende waarborgen (bijvoorbeeld adequaatheidsbesluit, deelname aan het Data Privacy Framework of SCC's in combinatie met landenonderzoek (DTIA)
53	IC-001	Inkoop & Contractmanagement	Facturatie	Alle facturen dienen als UBL 2.0 factuur-bestand te worden verstuurd naar digifactuur@han.nl t.n.v.: Hogeschool van Arnhem en Nijmegen T.a.v. Crediteurenadministratie Postbus 5375 6802 EJ Arnhem Nederland
54	IC-002	Inkoop & Contractmanagement	Facturatie	Facturen zonder Inkoopordernummer worden niet in behandeling genomen en niet geaccepteerd
55	IC-003	Inkoop & Contractmanagement	Facturatie	De aangeboden prijzen/tarieven zijn in Euro's afgerond en exclusief BTW.
56	IC-004	Inkoop & Contractmanagement	Facturatie	Inschrijver kan alleen kosten voor Dienstverlening in rekening brengen die vermeld staan op het prijzenblad
57	IC-007	Inkoop & Contractmanagement	Wet- en regelgeving	De totale dienstverlening moet (blijven) voldoen aan de Nederlandse wet- en regelgeving. Eventuele kosten van aanpassingen als gevolg van toekomstige wijzigingen in wet- en regelgeving worden gedragen door de leverancier.