Sociale Verzekeringsbank
Bijlage C Programma van Eisen
Deel II
Informatiebeveiliging en privacy

Arbodienstverlening PGB

Aanbestedingsnummer: EA2022010

Versie 1.1

S V B voor het leven
Sociale Verzekeringsbank

Inhoudsopgave

Paraaf voor akkoord:

1 Inleiding

In deze bijlage staan de Informatiebeveiligings- en privacyeisen met betrekking tot de gevraagde dienstverlening beschreven. Voordat wordt ingegaan op deze eisen wordt kort de positie van informatiebeveiliging binnen de SVB geschetst. Dit is van belang omdat u als leverancier deel gaat uitmaken van de informatieketen van de SVB.

Inschrijver dient elke pagina voor akkoord te paraferen en op de laatste pagina van deze Bijlage, het kader volledig in te vullen en te voorzien van een Origineel ingescande handgeschreven handtekening.

1.1 Achtergrond

De belangrijkste doelstelling van de SVB bij het uitvoeren van de sociale verzekeringen en in de zorg is ervoor te zorgen dat alle uitkeringen rechtmatig en tijdig worden uitbetaald. Om deze doelstelling te realiseren maakt de SVB gebruikt van mensen, processen, middelen en vertrouwelijke en persoonlijke informatie, die zij uitwisselt met klanten en ketenpartners ten behoeve van het uitvoeren van haar dienstverlening.

De SVB onderkent haar rol in de Nederlandse samenleving en neemt haar verantwoordelijkheid om de belangen van haar klanten en stakeholders goed te beschermen, en het vertrouwen wat haar gegund is waar te maken. Informatiebeveiliging, bedrijfscontinuïteit, cyber weerbaarheid en privacy maken integraal deel uit van de wijze waarop de SVB opereert.

1.2 Informatiebeveiligingsprincipes

Als onderdeel van het SVB informatiebeveiligings- en privacybeleid is een viertal informatiebeveiligings- en privacyprincipes vastgesteld welke de basis vormen voor de wijze waarop informatiebeveiliging, bedrijfscontinuïteit en privacy binnen de SVB worden vormgegeven:

I Wij **beschermen te allen tijde**, **de belangen van burgers** en andere stakeholders.

Wij zorgen dat we op ieder moment en op iedere plek in onze processen, de informatie van de burger op transparante en aantoonbare wijze beschermen en dat die informatie alleen toegankelijk is voor bevoegden, niet verloren kan gaan en/of ongewild wordt veranderd.

II Wij **gebruiken** alleen **informatie waarvoor** die **bedoeld** is en zijn daar transparant in.

Wij gebruiken de informatie van burgers niet voor andere zaken dan waar een rechtmatige grondslag voor is (zoals wettelijke grondslag of toestemming van de burger).

III Wij hebben **robuuste** en **betrouwbare processen en IT-systemen**.

Bij het ontwikkelen en het in standhouden van processen en IT-systemen, zorgen wij ervoor dat er afdoende maatregelen zijn genomen, die het belang van deze processen en systemen waarborgen.

IV Wij zijn **voorbereid** op onverwachte **verstoringen** van **onze dienstverlening**.

Wij zien alle verstoring die zich voordoen en hebben de organisatie voorbereid (processen, middelen en vaardigheden) om daar op een adequate wijze mee om te gaan, zodat de belangen van de stakeholders gewaarborgd zijn.

Bovenstaande principes zijn dan ook direct van toepassing op de wijze waarop de Opdrachtnemer haar werkzaamheden dient uit te voeren en moeten integraal verwerkt zijn in de werkwijze en processen van de Opdrachtnemer.

1.3 Informatiebeveiligingsbeleid

Het informatiebeveiligingsbeleid van de SVB is gebaseerd op de NEN-ISO/IEC 27001 norm en de NEN-ISO/IEC 27002 best-practice. Opdrachtnemer dient haar beveiligingsbeleid te baseren op de meest actuele versies van de NEN-ISO/IEC 27001 en de NENISO/ IEC 27002 of opvolgers hiervan, of een gelijkwaardige normering.

Paraaf voor akkoord:

De hoofdstukken H2 t/m H5 dienen ter verduidelijking van de eerder genoemde normen. In voorvallen waar H2 t/m H5 de genoemde normen afzwakken of tegenspreken prevaleren de genoemde normen altijd.

1.4 Wet- en regelgeving

De SVB is, onder meer, gehouden aan alle voorschriften uit relevante regelgeving waarbij de volgende wetten het meeste raakvlak hebben met informatiebeveiliging en privacy:

- AVG (Algemene Verordening Gegevensbescherming) – direct van toepassing op de leverancier.
- Wet en Regeling SUWI (Wet structuur uitvoeringsorganisatie werk en inkomen) – (onderdelen) alleen van toepassing indien expliciet opgenomen in dit programma van eisen.
- De BIO (Baseline Informatiebeveiliging Overheid). In het kader van ketenverantwoordelijkheid verwachten wij dit ook van Opdrachtnemers.

1.5 Basis Beveiligingsniveau (BBN)

Binnen de BIO wordt op basis van generieke schade en bedreigingen voor de Rijksoverheid, een onderscheid gemaakt in drie basisbeveiligingsniveau's, ook wel BBN's genoemd. De BBN's bouwen voort op het vorige niveau. Dus hoe hoger het niveau, hoe hoger de potentiële impact en hoe meer maatregelen.

De gevraagde dienstverlening moet minimaal geschikt zijn om informatie te verwerken op beveiligingsniveau BBN 2.

Deze BBN is van toepassing indien er vertrouwelijke informatie wordt verwerkt, mogelijke incidenten leiden tot bestuurlijke commotie, er onzekerheid bestaat of ook alle informatie van derden open is en de veiligheid van andere systemen afhankelijk is van de veiligheid van het eigen systeem.

Paraaf voor akkoord:

2 Eisen aan personeel van Opdrachtnemer

De Opdrachtnemer zet personeel in voor het uitvoeren van alle voorkomende werkzaamheden zoals deze zijn onderkend. De volgende eisen worden met betrekking tot de medewerkers van de Opdrachtnemer gesteld.

Eis	Omschrijving
IBP-2.1	Alle medewerkers van Opdrachtnemer die participeren in de levering van de gevraagde dienstverlening moeten aantoonbaar bekend zijn met de overeengekomen verplichtingen op het gebied van informatiebeveiliging en bescherming van persoonsgegevens.
IBP-2.2	Opdrachtnemer draagt zorg dat alle medewerkers die participeren in de levering van de gevraagde dienstverlening een geheimhoudingsovereenkomst ondertekenen en hier naar handelen.
IBP-2.3	Opdrachtnemer draagt zorg dat alle medewerkers die participeren in de levering van de gevraagde dienstverlening een Verklaring Omtrent Gedrag (VOG), of een gelijkwaardig document, hebben die geldig is tijdens de duur van de uitvoering van de werkzaamheden.

Paraaf voor akkoord:

3 Beveiliging van Diensten

3.1 Algemeen

Informatiebeveiliging moet als proces binnen de organisatie geborgd zijn om de informatie met de passende technische en organisatorische maatregelen te kunnen beveiligen. De gevraagde dienstverlening moet aan de volgende eisen voldoen.

Eis	Omschrijving
IBP-3.1.1	De gevraagde dienstverlening moet opgezet en geleverd worden vanuit het basisprincipe “Secure-by-Design” en “Privacy-by-design and default”.
IBP-3.1.2	Opdrachtnemer heeft informatiebeveiliging en bedrijfscontinuïteit aantoonbaar gestandaardiseerd, gestructureerd, continu en cyclus procesmatig (PDCA cyclus) in alle lagen van de organisatie (en voor zover van toepassing, betrokken toeleveranciers of onderaannemers) en gevraagde dienstverlening ingericht.
IBP-3.1.3	De gevraagde dienstverlening (incl. te gebruiken componenten) moet adequaat zijn beveiligd door het implementeren en onderhouden van een set van technische en organisatorische maatregelen welke de beschikbaarheid, integriteit en vertrouwelijkheid van de dienstverlening en de daarop opgeslagen en/of verwerkte informatie borgt op ten minste industriestandaard wijze.
IBP-3.1.4	Opdrachtnemer moet een procedure hebben, uitvoeren en de resultaten rapporteren voor het minimaal jaarlijks en bij significante wijzigingen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de gevraagde dienstverlening.
IBP-3.1.5	Voor het uitvoeren van onderhoud en/of aanpassingen moet aantoonbaar een wijzigingsproces gehanteerd worden (“change management”) waarbij de nadruk ligt op het voorkomen van beveiligingsincidenten, storingen of onderbrekingen tijdens het doorvoeren van veranderingen.
IBP-3.1.6	Opdrachtnemer dient zorg te dragen dat software welke gebruikt wordt als onderdeel van de gevraagde dienstverlening, altijd wordt ondersteund door de leverancier van de software en functioneert binnen de SVB-werkomgeving.
IBP-3.1.7	Opdrachtnemer dient de SVB voortdurend in staat te stellen om minimaal aan de eisen op BBN-2 niveau van de BIO te voldoen.
IBP-3.1.8	Opdrachtnemer treedt op als hoofdaannemer indien zij een of meerdere onderaannemers (waaronder een dochter of zusteronderneming) inschakelt. Opdrachtnemer is te allen tijde verantwoordelijk voor de borging van de overeengekomen eisen van de gevraagde dienstverlening en dient als aanspreekpunt voor de SVB.
IBP-3.1.9	De structuur van de beheerprocessen, de taken, verantwoordelijkheden en bevoegdheden zijn vastgesteld, belegd, gedocumenteerd en beschikbaar gesteld.

Paraaf voor akkoord:

3.2 Risicoanalyses

De wendbaarheid van de gevraagde dienstverlening komt voort uit de adequate wijze waarop risico's worden beheerst waardoor het makkelijker is om op korte termijn risico-gestuurde besluiten te nemen. De gevraagde dienstverlening moet aan de volgende eisen voldoen.

Eis	Omschrijving
IBP-3.2.1	Opdrachtnemer heeft procedures om het analyseren van risico's te borgen in het kader van de gevraagde dienstverlening (oa voor bouw- en implementatietrajecten en bij significante wijzigingen). De (opvolging van de) voor de SVB relevante (IB)-risico's en mitigerende maatregelen worden besproken en waar nodig belegd, opgevolgd en meegenomen in de met de SVB afgesproken rapportagecyclus.
IBP-3.2.2	Opdrachtnemer legt onderkende risico's vast in een register en deze wordt door Opdrachtnemer voorzien van de benodigde (borgings-)maatregelen ter mitigatie van de risico's.
IBP-3.2.3	Opdrachtnemer moet de SVB direct op de hoogte stellen van risico's die de classificatie "hoog" bestempeld krijgen.
IBP-3.2.4	Periodiek (minimaal eens per kwartaal) moet worden gerapporteerd over de status van de risico's en de bijbehorende (voortgang van de) mitigerende maatregelen.

3.3 Logische toegangsbeveiliging

Logische toegangsbeveiliging richt zich op het administreren en beheren van gebruikers en resources inclusief toegangsrechten en toegangscontrole. De gevraagde dienstverlening moet aan de volgende eisen voldoen.

Eis	Omschrijving
IBP-3.3.1	De ingezette logische toegangsbeveiligingsmiddelen moeten betrouwbare en effectieve mechanismen leveren voor het vastleggen en vaststellen van de identiteit van gebruikers, het toekennen van de rechten aan gebruikers, en het controleerbaar maken van het gebruik van deze middelen.
IBP-3.3.2	De gevraagde dienstverlening moet afdwingen dat gebruikers alleen toegang hebben tot informatie, beheertaken en speciale bevoegdheden voor zover dat voor de uitoefening van de werkzaamheden noodzakelijk is ("need to know", "need to use", "least privilege") en ze hiervoor herleidbaar geautoriseerd zijn (er is sprake van persoonlijke accounts).
IBP-3.3.3	De systemen van Opdrachtnemer voor wachtwoordbeheer behoren interactief te zijn en sterke wachtwoorden te waarborgen.
IBP-3.3.4	Opdrachtnemer is verantwoordelijk voor het periodiek (minimaal eens per kwartaal) controleren van de toegangsrechten van de eigen medewerkers die werkzaamheden uitvoeren ten behoeve van de gevraagde dienstverlening en legt hierover verantwoording af als onderdeel van de periodieke rapportage.

Paraaf voor akkoord:

3.4 Vulnerability management

Het tijdig informatie verkrijgen over technische kwetsbaarheden van de gebruikte informatiesystemen is van vitaal belang bij de beveiliging van de gevraagde dienstverlening. De mate waarin de organisatie blootstaat aan dergelijke kwetsbaarheden behoort te worden geëvalueerd en er behoren geschikte maatregelen te worden genomen voor de mitigatie van de daarmee samenhangende risico's. De gevraagde dienstverlening moet aan de volgende eisen voldoen.

Eis	Omschrijving
IBP-3.4.1	Opdrachtgever heeft procedures waardoor wordt geborgd dat continu naar nieuwe kwetsbaarheden en dreigingen wordt gezocht (vulnerability management) in het kader van regulier beheer (alle ICT-componenten) en bij in gebruik name van een nieuwe dienst/ict-component/significante wijziging.
IBP-3.4.2	De (opvolging van de) voor de SVB relevante bevindingen worden besproken en waar nodig belegd, opgevolgd en meegenomen in de met de SVB afgesproken rapportagecyclus.
IBP-3.4.3	Opdrachtnemer rapporteert periodiek (minimaal eens per kwartaal) over de resultaten van de kwetsbaarhedenscans en de daarbij behorende (voorgestelde) mitigerende maatregelen.

3.5 Patch management

Patch management is het proces dat ervoor zorgt dat alle componenten (ICT-systemen) ingezet voor de gevraagde dienstverlening systematisch voorzien worden van de vereiste patches. Het zorgt voor het verwerven, testen en installeren van patches. De gevraagde dienstverlening moet aan de volgende eisen voldoen.

Eis	Omschrijving
IBP-3.5.1	Patch management moet procesmatig, ondersteund door gestandaardiseerde en vastgestelde richtlijnen, worden uitgevoerd op alle ICT-systemen van de gevraagde dienstverlening en borgen dat de meest recente (beveiligings)patches zijn geïnstalleerd.
IBP-3.5.2	Indien een (beveiligings)patch beschikbaar is, moeten de risico's verbonden aan de installatie van de patch worden geëvalueerd en moet de patch getest worden alvorens deze op productiesystemen wordt toegepast.
IBP-3.5.3	Opdrachtnemer rapporteert periodiek (minimaal eens per kwartaal) over de resultaten van het patch management proces en de daarbij behorende (eventuele) afwijkingen en/of risico's.

Paraaf voor akkoord:

3.6 Security hardening

Security hardening is het proces dat ervoor zorgt dat alle componenten (ICT-systemen) ingezet voor de gevraagde dienstverlening op gestandaardiseerde wijze worden ingericht en structureel beheerd, waarbij de insteek is om de veiligheidsrisico's zoveel mogelijk te elimineren. De gevraagde dienstverlening moet aan de volgende eisen voldoen.

Eis	Omschrijving
IBP-3.6.1	Security hardening moet procesmatig, ondersteund door gestandaardiseerde en vastgestelde richtlijnen, worden uitgevoerd op alle ICT-systemen van de gevraagde dienstverlening.
IBP-3.6.2	Bij het vaststellen en toepassen van de security hardening richtlijnen moet minimaal onderscheid gemaakt worden tussen de volgende ICT componenten: ▪ Applicaties; ▪ Middleware en databases; ▪ Platformen / infrastructuur; ▪ Netwerken; en ▪ Connectiviteit
IBP-3.6.3	Opdrachtnemer hanteert internationaal erkende security hardening standaarden, zoals de CIS (Center of Internet Security) benchmarks, als basis voor het vaststellen van de security hardening richtlijn voor de ICT componenten.
IBP-3.6.4	Opdrachtnemer toetst periodiek (minimaal eens per kwartaal) alle ICT componenten op basis van de vastgestelde richtlijn en rapporteert de resultaten als onderdeel van de kwartaalrapportage. Geconstateerde afwijkingen worden hierin, na analyse, op basis van risico inschatting benoemd.

3.7 Penetratietesten

Met het uitvoeren van penetratietesten kan met een beperkte mate van zekerheid ingeschat worden in hoeverre de ICT componenten als onderdeel van de gevraagde dienstverlening kwetsbaar zijn voor inbraak. De gevraagde dienstverlening moet aan de volgende eisen voldoen.

Eis	Omschrijving
IBP-3.7.1	Penetratietesten moeten procesmatig en procedureel, ondersteund door richtlijnen, worden uitgevoerd op alle ICT componenten van de gevraagde dienstverlening.
IBP-3.7.2	Voor in gebruik name van een nieuwe dienst / ICT component of bij een significante wijziging, en minimaal jaarlijks, moet een penetratietest uitgevoerd worden en moeten de bevindingen opgelost worden.
IBP-3.7.3	Opdrachtnemer rapporteert de resultaten van de penetratietesten direct aan de SVB en legt vervolgens periodiek (minimaal eens per kwartaal) verantwoording af over de opvolging van de bevindingen.
IBP-3.7.4	De SVB heeft het recht om een penetratietest uit te laten voeren om de beveiliging te testen in het kader van de gevraagde dienstverlening. De SVB kiest hierbij zelf een onafhankelijk en algemeen erkend bureau dat de testen uitvoert. De (opvolging van de) voor de SVB relevante bevindingen worden besproken en waar nodig belegd, opgevolgd en meegenomen in de met de SVB afgesproken rapportagecyclus.

Paraaf voor akkoord:

3.8 Beveiliging webapplicaties

Het beveiligen van webapplicaties heeft tot doel om te waarborgen dat webapplicaties functioneren zoals is beoogd, ingericht zijn volgens specifieke beleidsuitgangspunten van de organisatie en voldoen aan de eisen die door de organisatie zijn gesteld ten aanzien van de kwaliteitsaspecten vertrouwelijkheid, integriteit, beschikbaarheid en controleerbaarheid. De gevraagde dienstverlening moet aan de volgende eisen voldoen.

Eis	Omschrijving
IBP-3.8.1	Bij het ontwikkelen, implementeren en beheren van een webapplicatie moet gebruik gemaakt worden van Secure Software Development technieken om de beveiliging van de webapplicatie te borgen.
IBP-3.8.2	De gevraagde dienstverlening moet voldoen aan de NCSC ICT-Beveiligingsrichtlijnen voor Webapplicaties dan wel de logische opvolgers daarvan. (https://www.ncsc.nl/documenten/publicaties/2019/mei/01/beleids--en-beheersingsrichtlijnen-voor-de-ontwikkeling-van-veilige-software).
IBP-3.8.3	Opdrachtnemer moet de OWASP top tien (https://owasp.org/www-project-top-ten/) dan wel de logische opvolgers daarvan, structureel hanteren om meest kritische beveiligingsrisico's binnen een webapplicatie te vermijden.
IBP-3.8.4	De cryptografische beveiligingsvoorzieningen van de gevraagde dienstverlening moeten voldoen aan de NCSC ICT-Beveiligingsrichtlijnen voor Transport Layer Security (TLS), dan wel logische opvolgers daarvan (https://www.ncsc.nl/onderwerpen/verbindingsbeveiliging/documenten/publicaties/2021/januari/19/ict-beveiligingsrichtlijnen-voor-transport-layer-security-2.1).

Paraaf voor akkoord:

3.9 Infrastructurele beveiligingseisen

De doelstelling is te waarborgen dat de infrastructuur werkt zoals beoogd, ingericht is volgens specifieke beleidsuitgangspunten, en voldoet aan de eisen ten aanzien van de kwaliteitsaspecten vertrouwelijkheid, integriteit, beschikbaarheid en controleerbaarheid. De gevraagde dienstverlening moet aan de volgende eisen voldoen.

Eis	Omschrijving
IBP-3.9.1	Als onderdeel van de architectuur van de gevraagde dienstverlening moet netwerksegmentatie / zonering conform een “defense in depth” strategie worden toegepast.
IBP-3.9.2	De componenten die deel uitmaken van de gevraagde dienstverlening en de diensten die hierover aangeboden worden moeten worden beschermd tegen aanvallen op de beschikbaarheid, integriteit en vertrouwelijkheid.
IBP-3.9.3	In de ICT infrastructuur moeten signaleringsfuncties (registratie/logging en detectie) actief, efficiënt, effectief en beveiligd ingericht zijn.
IBP-3.9.4	De loggings- en detectie-informatie (registraties en alarmeringen) en de condities van de beveiliging van ICT systemen moeten regelmatig worden gemonitord (bewaakt, geanalyseerd) en de bevindingen periodiek gerapporteerd als onderdeel van het informatiebeveiliging incidentenproces.
IBP-3.9.5	Indien mobiele apparatuur in gebruik door personeel gegevens bevat gerelateerd aan de Prestatie die door Opdrachtgever en/of Opdrachtnemer als vertrouwelijk is geclassificeerd, dient Opdrachtnemer in ieder geval deze gegevens te versleutelen middels cryptografische toepassingen, waarbij uitsluitend algoritmes en instellingen worden gebruikt met de duiding goed uit de meest actuele versie van het Nationaal Cyber Security Centrum (NCSC) document Richtlijnen voor Transport Layer Security (TLS).
IBP-3.9.6	De Opdrachtnemer verwijdert media e/o apparatuur aantoonbaar op een veilige en beveiligde manier als ze niet langer nodig zijn, overeenkomstig formele procedures.
IBP-3.9.7	De Opdrachtnemer behoort beveiligde ontwikkelomgevingen vast te stellen en passend te beveiligen voor verrichtingen op het gebied van systeemontwikkeling en integratie, die betrekking hebben op de gehele levenscyclus van de systeemontwikkeling.

Paraaf voor akkoord:

3.10 Cloud

De veiligheid van de SVB gegevens is van kritiek belang bij het gebruik van dienstverlening die vanuit “de Cloud” wordt aangeboden, waarbij er in dezen vanuit wordt gegaan dat vertrouwelijke informatie en/of persoonsgegevens onderdeel zijn van deze gegevens. Het is dan ook belangrijk om naast de al gestelde eisen, een aantal specifieke eisen voor Cloud leveranciers te stellen. De gevraagde dienstverlening moet aan de volgende eisen voldoen.

Eis	Omschrijving
IBP-3.10.1	Verwerking van (waaronder toegang tot) data van de SVB moet uitsluitend plaatsvinden binnen de Europese Economische Ruimte (Europese Unie, Noorwegen, Liechtenstein, IJsland).
IBP-3.10.2	Alle koppelingen tussen applicaties (interoperabiliteit) moet op basis van open standaarden plaatsvinden en worden standaard via de SVB koppelpunten geleid.
IBP-3.10.3	Opdrachtnemer moet garanderen en aantonen dat de SVB gegevens logisch en functioneel gescheiden zijn van de overige afnemers.
IBP-3.10.4	De gevraagde dienstverlening biedt een oplossing om vertrouwelijke en/of gevoelige gegevens versleuteld op te slaan waarbij gebruik gemaakt wordt van de geldende ‘best practices’ (afhankelijk van de stand der techniek) m.b.t. versleuteling.
IBP-3.10.5	De encryptie sleutels die gebruikt worden voor het versleutelen van de gegevens moeten adequaat beheerd worden door de Opdrachtnemer waarbij de SVB inzicht wil hebben in het beheer en gebruik van de encryptiesleutels. De bij de Opdrachtnemer toegepaste encryptie sleutels voor het encrypten van de data binnen de gevraagde dienstverlening moeten per direct ingetrokken of onbruikbaar kunnen worden gemaakt.

Paraaf voor akkoord:

4 Privacy

De Algemene Verordening Gegevensbescherming (AVG) beschermt de grondrechten en de fundamentele vrijheden van natuurlijke personen en met name hun recht op bescherming van persoonsgegevens. In dit overzicht zijn niet de eisen herhaald die zowel van toepassing zijn op Privacy als op Informatiebeveiliging; deze zijn reeds opgenomen in hoofdstuk 3. De gevraagde dienstverlening moet aan de volgende eisen voldoen.

Eis	Omschrijving
IBP-4.1	De gevraagde dienstverlening moet gedurende de gehele looptijd van de overeenkomst voldoen aan de algemene vigerende wet- en regelgeving van de Nederlandse overheid, waaronder de AVG (Algemene Verordening Gegevensbescherming).
IBP-4.2	In lijn met Verwerkersovereenkomst moet Opdrachtnemer de van de SVB ontvangen persoonsgegevens uitsluitend op basis van schriftelijke instructies van de SVB verwerken voor doeleinden die rechtstreeks voortvloeien uit de werkzaamheden die partijen zijn overeengekomen, en zal Opdrachtnemer de persoonsgegevens dus niet gebruiken voor: ▪ Het uitvoeren van testen; en ▪ Het uitvoeren van data-analyses.
IBP-4.3	Daar waar de SVB geen volledige toegang heeft tot de persoonsgegevens moet Opdrachtnemer de SVB ondersteunen bij verzoeken tot inzage, correctie en eventueel het wissen van persoonsgegevens.
IBP-4.4	De gevraagde dienstverlening moet de mogelijkheid bieden om gegevenselementen die niet strikt noodzakelijk zijn voor latere verwerkingen of waarvoor geen doelbinding/rechtsgrond aanwezig is te verwijderen of te verbergen. In overleg met arbodienst zal op procesniveau vastgesteld worden welke gegevens zij nodig hebben voor het uitvoeren van de verschillende processen binnen de dienstverlening. Hierbij zal toegezien worden dat gegevens slechts eenmalig worden uitgewisseld.
IBP-4.5	Encryptie moet door Opdrachtnemer worden toegepast als een van de Privacy by design maatregelen indien er sprake is van: 1. Transport van persoonsgegevens over openbare of semiopenbare dat infrastructuur (internet, e-mail, extranet etc.). 2. Opslag en/of transport van persoonsgegevens op locaties en/of media waarbij de fysieke en/of logische beveiligingsmaatregelen ontoereikend worden geacht.
IBP-4.6	Bij het toepassen van data-protection-by default door de Opdrachtnemer moeten tenminste de volgende aspecten meegewogen worden: 1. Gedurende het systeemontwikkelproces moet continue rekening gehouden worden met de privacy van betrokkene. De belangen en privacy van betrokkene dienen centraal te staan. Bijvoorbeeld er is geen opt-out regime, maar opt-in: pas als iemand zich ergens voor heeft aangemeld ontvangt hij informatie (opt-in), niet het automatisch ontvangen totdat het wordt stopgezet (opt-out). 2. Bij het inrichten van autorisatierollen moet rekening gehouden worden met privacy en worden alleen die persoonsgegevens getoond die een medewerker nodig heeft voor zijn functie. 3. Beperk zoekfunctionaliteit m.b.t. persoonsgegevens en geef alleen zoekresultaten weer na het invoeren van een aantal persoonsgegevens. 4. Pas whitelisting toe voor het opvragen van persoonsgegevens. De sterkte van whitelisting is afhankelijk van de implementatie van de whitelist. Een goede toepassing is dat de whitelist wordt samengesteld door een mechanisme/tooling die onafhankelijk is van de gebruiker (bv. een workflow-systeem waarmee de gebruiker alleen toegang krijgt tot persoonsgegevens van de betrokkene waar hij op dat moment mee bezig is).
IBP-4.7	Voor de gevraagde dienstverlening moet per type informatie door SVB goedgekeurde bewaartermijnen kunnen worden ingesteld.

Paraaf voor akkoord:

5 Uitvoeringsaspecten

5.1 Beveiligingsincidenten en datalekken

Een beveiligingsincident is iedere handeling in strijd met het vastgestelde informatiebeveiligingsbeleid (van Opdrachtnemer en/of de SVB), of een gebeurtenis, met (mogelijk) nadelige gevolgen voor de beschikbaarheid, integriteit en/of vertrouwelijkheid van systemen en/of informatie, die vallen onder de verantwoordelijkheid en/of het beheer van de SVB en/of Opdrachtnemer. De gevraagde dienstverlening moet aan de volgende eisen voldoen.

Eis	Omschrijving
IBP-5.1.1	Opdrachtnemer meldt informatiebeveiligingsincidenten onverwijld per email bij de SVB Servicedesk, op het emailadres: servicedesk@svb.nl.
IBP-5.1.2	Opdrachtgever heeft monitoring-, meld- en responsprocedures geïmplementeerd (en evalueert periodiek de effectiviteit daarvan) om informatiebeveiligingsincidenten (waaronder datalekken m.b.t. persoonsgegevens) te detecteren, melden en de gevolgen daarvan te mitigeren.
IBP-5.1.3	Opdrachtnemer moet volledige medewerking geven bij het onderzoeken en oplossen van het informatiebeveiligingsincident en stelt, indien gevraagd, alle informatie met betrekking tot het incident ter beschikking aan de SVB.

5.2 Controle en audits

Ter ondersteuning van de eisen die de SVB stelt aan haar Opdrachtnemer, moet gedurende de looptijd van de overeenkomst met de Opdrachtnemer een aantal controles en/of audits uitgevoerd worden. De gevraagde dienstverlening moet aan de volgende eisen voldoen.

Eis	Omschrijving
IBP-5.2.1	SVB heeft het recht om bij Opdrachtnemer een onderzoek (of audit) in te stellen met betrekking tot de naleving van de overeengekomen verplichtingen aangaande de gevraagde dienstverlening. SVB kan het onderzoek (minimaal één keer per jaar) zelf uitvoeren of laten uitvoeren door onafhankelijke deskundigen.
IBP-5.2.2	Minimaal jaarlijks levert Opdrachtnemer een recente formele audit-verklaring die past bij de aard van de gevraagde dienstverlening (zoals een ISO27001:2017 / ISAE 3000 type 2 / SOC 2 type 2 of gelijkwaardig) op, die is afgegeven door een onafhankelijke geaccrediteerde auditor en waarmee de opzet, het bestaan en de werking van een passend stelsel van beveiligingsmaatregelen ten aanzien van de gevraagde dienstverlening wordt aangetoond.

Paraaf voor akkoord:

5.3 Overleg & rapportage

Als onderdeel van de besturing van de door Opdrachtnemer geleverde dienstverlening vindt regulier overleg plaats tussen de SVB en Opdrachtnemer en levert Opdrachtnemer periodiek rapportages op. De gevraagde dienstverlening moet aan de volgende eisen voldoen.

Eis	Omschrijving
IBP-5.3.1	Opdrachtnemer stelt een vaste contactpersoon aan die voor de gevraagde dienstverlening verantwoordelijk is voor zowel informatiebeveiliging als privacy.
IBP-5.3.2	Gestructureerd en periodiek (minimaal eens per kwartaal) overleg tussen Opdrachtnemer en SVB moet plaatsvinden om zowel de informatiebeveiligingsrapportages als (eventuele) issues te bespreken.
IBP-5.3.3	Opdrachtnemer moet zorgen voor een rapportage waarmee verantwoording wordt afgelegd over de mate van invulling en effectiviteit van de getroffen beveiligingsmaatregelen en het gerealiseerde beveiligingsniveau (inclusief privacy) binnen de scope van de geleverde dienstverlening.
IBP-5.3.4	Elk kwartaal moeten onderstaande rapportage-vereisten worden ingevuld (specifiek voor de geleverde dienstverlening): ▪ Een overzicht van de beveiligingsincidenten (inclusief datalekken) inclusief trends, evaluaties en (root cause) analyses; ▪ Rapportages van risico's, kwetsbaarheden (vulnerability scan resultaten), patch management, hardening afwijkingen en voortgangsrapportages over bijbehorende remediation plannen; en Analyse van de logging en monitoring informatie.
IBP-5.3.5	Jaarlijks moeten onderstaande rapportage-vereisten worden ingevuld (specifiek voor de geleverde dienstverlening): ▪ De status, handhaving en effectiviteit van de geïmplementeerde maatregelen; ▪ Overzicht van afwijkingen ten opzichte van beleid of contract; en ▪ Overzicht van de risico acceptaties.

6 Ondertekening

Ondergetekende verklaart volledig en onvoorwaardelijk te voldoen aan de in deze Bijlage opgenomen eisen:

Bedrijfsnaam Inschrijver: ……

Plaats: ……. Datum:……

Naam ondergetekende: …….. Functie:……

Handtekening: ……

Paraaf voor akkoord: