Programma van eisen – Informatiebeveiliging en privacy

Classificatie: Intern

Niets uit dit document mag zonder schriftelijke toestemming vooraf van de Sociale Verzekeringsbank worden verveelvoudigd, openbaar gemaakt of voor andere doelstellingen gebruikt worden dan het indienen van een inschrijving voor deze aanbesteding.

Europese aanbesteding Beheer V&O informatiesysteem

Versie 1.0

Paraaf:

Inhoudsopgave

Paraaf:

1 Inleiding

In deze bijlage staan de Informatiebeveiligingseisen 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 Opdrachtnemer deel gaat uitmaken van de informatieketen van de SVB.

1.1 Vereiste

Deelnemer 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.

1.2 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, cyberweerbaarheid en privacy maken integraal deel uit van de wijze waarop de SVB opereert.

1.3 Informatiebeveiligingsprincipes

Als onderdeel van het SVB informatiebeveiligingsbeleid is een viertal informatiebeveiligingsprincipes 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.

Paraaf:

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.

1.4 Informatiebeveiligingsbeleid

Het informatiebeveiligingsbeleid van de SVB is gebaseerd op de NEN-ISO/IEC 27001 norm en de NEN-ISO/IEC 27002 best-practice.

Eis	*Omschrijving*
IBP-1.1	Wederpartij dient haar beveiligingsbeleid te baseren op de meest actuele versies van de NEN-ISO/IEC 27001 en de NEN-ISO/ IEC 27002 of opvolgers hiervan, of een gelijkwaardige normering. Tevens dient Opdrachtnemer, of minimaal dat deel van de organisatie wat betrokken is bij de Dienstverlening aan de SVB, NEN-ISO27001 gecertificeerd te zijn.

1.5 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 Opdrachtnemer.
- 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.

Het Informatiebeveiliging- en privacy beleid van de SVB zelf is gebaseerd op de BIO (Baseline Informatiebeveiliging Overheid).

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

Paraaf:

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 bekend zijn met de verantwoordelijkheid op het gebied van Informatiebeveiliging en privacy die als onderdeel van zijn/haar rol van toepassing zijn.
IBP-2.2	Opdrachtnemer draagt zorg dat alle medewerkers die participeren in de levering van de gevraagde Dienstverlening een geheimhoudingsovereenkomst ondertekenen en hiernaar handelen.
IBP-2.3	Opdrachtnemer draagt zorg dat alle medewerkers die participeren in de levering van de gevraagde Dienstverlening aan de SVB, bij indiensttreding bij de Opdrachtnemer een Verklaring Omtrent Gedrag (VOG), of een gelijkwaardig document, hebben overlegd, die niet ouder is dan 12 maanden. De kosten van de VOG zijn voor rekening van de Opdrachtnemer.
IBP-2.4	Bij het betreden van een locatie van de SVB dienen medewerkers van of namens de Opdrachtnemer zich altijd te kunnen legitimeren met een wettelijk geldig legitimatiebewijs.
IBP-2.5	Opdrachtnemer heeft vastgelegd wat de verantwoordelijkheden en rollen zijn op het gebied van Informatiebeveiliging binnen haar organisatie.
IBP-2.6	Alle medewerkers van Opdrachtnemer en, voor zover relevant, contractanten behoren een passende bewustzijnsopleiding en -training te krijgen en regelmatige bijscholing van beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie.
IBP-2.7	Medewerkers van of namens Opdrachtnemer betreden alleen onder begeleiding de SVB-locaties.

Paraaf:

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'.
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 gevraagde Dienstverlening ingericht.
IBP-3.1.3	De gevraagde Dienstverlening 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.
IBP-3.1.4	Opdrachtnemer moet een procedure hebben, uitvoeren en de resultaten rapporteren voor het op gezette tijdstippen 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 die 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 garandeert testgegevens, betrokken bij de Dienstverlening, aantoonbaar zorgvuldig te kiezen, beschermen, controleren, en vernietigen na gebruik.
IBP-3.1.8	Opdrachtnemer heeft voor het aanvaardbaar gebruik van: ▪ informatie, en ▪ van bedrijfsmiddelen die samenhangen met informatie, en ▪ informatie verwerkende faciliteiten, regels geïdentificeerd, gedocumenteerd en geïmplementeerd.
IBP-3.1.9	Voor kantoren, ruimten en faciliteiten behoort fysieke beveiliging te worden ontworpen en toegepast. Beveiligde gebieden behoren te worden beschermd door passende toegangsbeveiliging om ervoor te zorgen dat alleen bevoegd personeel toegang krijgt.

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 moet structureel risicoanalyses uitvoeren in het bouw- en implementatietraject, als onderdeel van de PDCA-cyclus, bij grote onderhoudstrajecten, en bij significante wijzigingen in de gevraagde Dienstverlening.

Paraaf:

Eis	*Omschrijving*
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.
IBP-3.3.3	De gevraagde Dienstverlening moet, om het toegangsproces voor de SVB-medewerkers te faciliteren (Single Sign On), koppelen aan de IDaaS (Identity as a Service) dienst van de SVB waarbij de koppeling op basis van open standaarden moet worden vormgegeven.
IBP-3.3.4	Voor applicaties die vereisen dat een set van identiteitsinformatie van gebruikers in het systeem aanwezig is, moet gebruik worden gemaakt van automatische provisioning. De SVB is hierbij verantwoordelijk voor het vaststellen van de filtering van de accountattributen die geprovisioned worden.
IBP-3.3.5	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.

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	Het beheer van kwetsbaarheden (vulnerability management) moet procesmatig en regulier (minimaal eens per kwartaal) worden uitgevoerd op alle ICT-componenten behorend bij de gevraagde Dienstverlening.

Paraaf:

Eis	*Omschrijving*
IBP-3.4.2	Voor in gebruik name van een nieuwe dienst/ICT-component en bij een significante wijziging moet een kwetsbaarhedenscan uitgevoerd worden en moeten de bevindingen opgelost worden.
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

Patchmanagement 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	Patchmanagement moet procesmatig, ondersteund door gestandaardiseerde en vastgestelde richtlijnen, worden uitgevoerd op alle ICT-componenten van de gevraagde Dienstverlening en borgen dat de meest recente (beveiligings)patches zijn geïnstalleerd, conform leveranciersadviezen.
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 patchmanagementproces en de daarbij behorende (eventuele) afwijkingen en/of risico's.

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. ICT-componenten waarvoor geen internationaal erkende security benchmarks beschikbaar zijn, zullen worden geconfigureerd conform de beveiligingsrichtlijnen van de leverancier van de apparatuur.

Paraaf:

Eis	*Omschrijving*
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. Opdrachtnemer verleent medewerking aan een tevoren schriftelijk aangekondigde penetratietest.
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.

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 (September 2015), dan wel de logische opvolgers daarvan (https://www.ncsc.nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-webapplicaties.html).
IBP-3.8.3	Opdrachtnemer moet minimaal de OWASP top tien (https://www.owasp.org/index.php/Top_10-2017_Top_10) 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/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-transport-layer-security-tls.html).

Paraaf:

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	De gevraagde Dienstverlening moet op dit moment alleen vanuit het SVB-netwerk toegankelijk worden gemaakt voor de SVB-medewerkers, en moet in de nabije toekomst via publiek internet (met mogelijkerwijs een cloud access security tussenlaag) toegankelijk kunnen worden gemaakt.
IBP-3.9.6	Opdrachtnemer draagt zorg dat de netwerkverbindingen zowel fysiek als logisch zijn beveiligd tegen ongeautoriseerde toegang door derden. Hiertoe worden binnen de branche gebruikelijke maatregelen toegepast. Opdrachtnemer dient op aanvraag van de SVB inzichtelijk te maken welke maatregelen geïmplementeerd zijn en hoe deze gecontroleerd worden.

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 ervan uit 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 data 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	Wederpartij zorgt er voor en zal aantonen 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 in eigendom en beheer zijn bij de SVB. De bij de Opdrachtnemer toegepaste encryptie sleutels moeten per direct ingetrokken of onbruikbaar kunnen worden gemaakt.

Paraaf:

Eis	*Omschrijving*
IBP-3.10.6	In het kader van dataportabiliteit moet de Opdrachtnemer de volgende voorzieningen direct ter beschikking stellen voor het exporteren van data (na beëindiging van de Dienstverlening): ▪ SaaS – Data moet beschikbaar zijn in een voor de SVB bruikbaar format zoals CSV, Excel (xlsx) en PDF. In het geval er sprake is van aanlevering van documenten tijdens gebruik van de dienst, dan moet het originele/oorspronkelijke format van het document (inclusief mappenstructuren) beschikbaar zijn. ▪ PaaS – Te exporteren data moet minimaal de applicatie, applicatie-data en gebruikersgegevens bevatten. ▪ IaaS – Data moet beschikbaar zijn op 'Virtual Machine' niveau, waarbij de volgende formaten worden geaccepteerd: open virtualization format (OVF, OVA), of een binnen de SVB geaccepteerde specifieke virtual hostingstandaard.

Paraaf:

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 de 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 overeenkomen.
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.
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	Opdrachtnemer dient de integriteit en vertrouwelijkheid van het over zijn netwerk getransporteerde gesprek/verkeer van de SVB te waarborgen. Aan de hand van fysieke als wel logische maatregelen voorkomt Opdrachtnemer de mogelijkheid tot het afluisteren van netwerkverbindingen en borgt zij de integriteit van het verkeer.

Paraaf:

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, waaronder maar niet beperkt tot datalekken, direct en in ieder geval binnen 24 uur per email bij de SVB servicedesk, op het emailadres: servicedesk@svb.nl.
IBP-5.1.2	In het geval van een Informatiebeveiligingsincident moet de Opdrachtnemer redelijkerwijs maatregelen treffen om de gevolgen en de schade te beperken voortkomend uit het Incident.
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 het contract 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 in dit document opgenomen verplichtingen aangaande de gevraagde Dienstverlening. SVB kan het onderzoek 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 ISAE 3000 rapportage op basis van één of meerdere SOC2 – Trusted Services Principes, 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.

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 rapportages als (eventuele) issues te bespreken.

Paraaf:

Eis	*Omschrijving*
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), patchmanagement, 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 acceptatie.

5.4 Behandeling van log-data

Met betrekking tot de behandeling van log-data dienen er afspraken gemaakt te worden tussen de SVB en de Opdrachtnemer. Afhankelijk van dienst die de SVB afneemt, gelden er de volgende eisen:

Eis	*Omschrijving*
IBP-5.4.1	Als de SVB gebruik maakt van een door de Opdrachtnemer geleverde en beheerde applicatie en/of dienst, dan dient de Opdrachtnemer de log-events met betrekking tot het gedrag van de SVB-gebruikers en de toegang en handeling op de SVB-data binnen die dienst en/of applicatie beschikbaar te stellen aan de SVB. Dit middels een nader overeen te komen timing, gangbaar format en overdracht-mechanisme tussen de SVB en de Opdrachtnemer waarbij een adequate bescherming van deze data wordt toegepast.
IBP-5.4.2	Als de SVB eigen componenten (hardware, software en elke combinatie hiervan) plaatst in de door de Opdrachtnemer beheerde en aan SVB beschikbaar gestelde omgeving, dan dient de Opdrachtnemer alle log-events met betrekking tot deze SVB-componenten aan de SVB beschikbaar te stellen. Dit middels een nader overeen te komen timing, gangbaar format en overdracht-mechanisme tussen de SVB en de Opdrachtnemer waarbij een adequate bescherming van deze data wordt toegepast.

Paraaf:

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: