EA2022028 Identity and Access Management: Bijlage G – Programma van Eisen IBP

Programma van Eisen

Informatiebeveiliging en Privacy

Inhoudsopgave

1 Inleiding

In deze bijlage staan de Informatiebeveiligings- & Privacy (IB&P) eisen met betrekking tot de geleverde Oplossing / Dienstverlening beschreven. Voordat wordt ingegaan op deze eisen wordt kort de positie van IB&P binnen de Sociale Verzekeringsbank (SVB) geschetst. Dit is van belang omdat u als dienstverlener deel gaat uitmaken van de informatieketen van de SVB.

1.1 Achtergrond

De belangrijkste doelstelling van de SVB bij het uitvoeren van haar taken m.b.t. de sociale verzekeringen en in de zorg is ervoor zorg te dragen dat alle uitkeringen rechtmatig en tijdig worden uitbetaald. Om deze doelstelling te realiseren maakt de SVB gebruikt van mensen, processen, middelen en persoonlijke en/of vertrouwelijke 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 belanghebbende 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 Informatiebeveiliging & Privacy (IB&P) principes

Als onderdeel van het SVB informatiebeveiliging- en privacybeleid zijn een viertal principes 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 burgers, medewerkers en andere stakeholders 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 we zijn daar transparant in.
Wij gebruiken de informatie van burgers en medewerkers niet voor andere zaken dan waar een wettelijke grondslag voor is (zoals de uitvoering van een publieke taak 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 en de continuïteit van onze processen en systemen waarborgen.

IV Wij zijn **voorbereid** op onverwachte **verstoringen van onze Dienstverlening**.
Wij zien alle verstoringen 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 Informatiebeveiliging & Privacybeleid

Het informatiebeveiliging & Privacybeleid van de SVB, hierna te noemen opdrachtgever, is gebaseerd op de NEN-ISO/IEC 27001 norm en de NEN-ISO/IEC 27002 best practices. Opdrachtnemer dient haar IB&P-beleid te baseren op de meest actuele versies van hiervoor genoemde standaarden of opvolgende c.q. gelijkwaardige normeringen.

1.4 Relevante wet- en regelgeving

De opdrachtgever is, onder meer, gehouden aan alle voorschriften uit relevante regelgeving waarbij de volgende wetten het meeste raakvlak hebben met Informatiebeveiliging en Privacy:

- **Van algemene aard** - Nederlandse wetgeving met bijbehorende jurisprudentie (AVG, Archiefwet, enz.).
- **Vanwege het uitvoeren van betalingen** - SWIFT.
- **Vanwege het klant zijn van DigiD** - DigiD-normenkader.
- **Vanwege het zijn van een zelfstandig bestuursorgaan (ZBO) -** Baseline Informatiebeveiliging Overheid (BIO), Wet structuur uitvoeringsorganisatie werk en inkomen (SUWI) en Forum voor Standaardisatie.

1.5 Basis Beveiligings Niveau (BBN)

Binnen de Baseline Informatiebeveiliging Overheid (BIO) wordt op basis van generieke schade en bedreigingen voor de Rijksoverheid, een onderscheid gemaakt in drie basis beveiligingsniveaus, 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 c.q. stringentere maatregelen er geïmplementeerd dienen te worden.

De geleverde Oplossing / Dienstverlening dient minimaal geschikt te zijn om informatie te verwerken op beveiligingsniveau BBN2. BBN2 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 wanneer de veiligheid van andere systemen afhankelijk is van de veiligheid van het eigen systeem.

1.6 Categorisering eisen

In deze bijlage zijn de navolgende prefixen gebruikt ter categorisering van de eisen:

Prefix	Type eis
IBPA	Algemeen (generiek)
IBPB	T.a.v. het beheer (zowel bij intern, extern als gemeenschappelijk beheer)
IBPD	T.a.v. het ontwerp en/of de inrichting van de Oplossing
IBPP	T.a.v. ingehuurd personeel

2 Generieke eisen ten aanzien van personeel van de Opdrachtnemer

Inzet door de Opdrachtnemer van personeel dient aan hieronder staande eisen te worden voldaan:

Eis	Omschrijving
IBPP-2.1	Opdrachtnemer is voor opdrachtgever altijd eerste aanspreekpunt en eindverantwoordelijk voor de borging van de overeengekomen verplichtingen met betrekking tot de Dienstverlening ook indien zij één of meerdere onderaannemers (waaronder een dochter of zusteronderneming) inschakelt.
IBPP-2.2	Medewerkers van de Opdrachtnemer die in aanraking komen met vertrouwelijke informatie van de opdrachtgever dienen een geheimhoudingsovereenkomst (NDA) te hebben ondertekend en op basis hiervan te handelen.
IBPP-2.3	Medewerkers van de Opdrachtnemer die participeren in de levering van de Dienstverlening dienen te beschikken over een relevante geldige Verklaring Omtrent Gedrag (VOG) of een gelijkwaardig ander document welke niet ouder is dan 36 maanden. De kosten van de VOGs en de administratie hieromtrent zijn voor rekening van de Opdrachtnemer.
IBPP-2.4	Medewerkers van de Opdrachtnemer dienen bij het betreden van locaties van de opdrachtgever zich altijd te kunnen legitimeren met een wettelijk geldig legitimatiebewijs.
IBPP-2.5	Medewerkers die namens en/of in opdracht van Opdrachtnemer participeren in de levering van de Dienstverlening dienen aantoonbaar bekend te zijn met de contractueel overeengekomen verplichtingen op het gebied van Informatiebeveiliging en Privacy.
IBPP-2.6	Opdrachtnemer dient vastgelegd te hebben wat de rollen, taken en verantwoordelijkheden van haar medewerkers zijn op het gebied van Informatiebeveiliging en Privacy in relatie tot de geleverde Dienstverlening.
IBPP-2.7	Medewerkers van de Opdrachtnemer en eventuele onderaannemer(s) dienen een passende bewustzijnsopleiding en/of -training te hebben gehad en regelmatige bijscholing van organisatie beleidsregels en procedures te krijgen, voor zover relevant voor hun functie / rol in relatie tot de geleverde Dienstverlening.

3 Generieke eisen ten aanzien van Informatiebeveiliging (IB)

3.1 Algemeen

Informatiebeveiliging gaat over de beschikbaarheid, integriteit en vertrouwelijkheid van data / informatie en heeft tot doel om informatie met passende maatregelen te beschermen / beveiligen. Het geleverde dient op dit onderdeel minimaal aan de hieronder staande eisen te voldoen:

Eis	Omschrijving
IBPA-3.1.1	De geleverde Oplossing dient minimaal te voldoen aan de BBN2-eisen zoals beschreven in de laatste versie van de Baseline Informatiebeveiliging Overheid (BIO) echter wanneer binnen de Oplossing data wordt opgeslagen of verwerkt met een hoge classificering dan BBN2 dienen minimaal de betrokken onderdelen van de Oplossing deze BBN-classificering te ondersteunen.
IBPA-3.1.2	De geleverde Oplossing dient adequaat te zijn beveiligd middels een set van maatregelen gebaseerd op algemeen geaccepteerde standaarden, welke de beschikbaarheid, integriteit en vertrouwelijkheid van de Oplossing (inclusief de toegepaste ICT-componenten) en de daarop opgeslagen en/of verwerkte informatie borgt.
IBPA-3.1.3	De geleverde Oplossing dient alleen (software) componenten te bevatten welke worden ondersteund door de fabrikant(en), dan wel de eigenaar van de source code en correct en veilig te functioneren binnen en/of in samenwerking met de omgeving van de opdrachtgever.
IBPA-3.1.4	(Eventueel) betrokken gegevens bij de realisatie van een Oplossing en in het bijzonder persoonsgegevens dienen zorgvuldig te zijn gekozen, te worden beschermd en vernietigd indien niet meer noodzakelijk.
IBPA-3.1.5	Opdrachtnemer dient ervoor te zorgen dat ten aanzien van het veilig gebruik van informatie, bedrijfsmiddelen en/of faciliteiten die samenhangen met de Dienstverlening gebruiksregels zijn geïdentificeerd, gedocumenteerd en geïmplementeerd.
IBPA-3.1.6	Opdrachtnemer dient ervoor te zorgen dat met betrekking tot haar kantoren, ruimten en/of faciliteiten en thuiswerkplekken, zover als betrokken bij de opdracht, passende beveiligingsmaatregelen zijn geïmplementeerd.
IBPD-3.1.7	De geleverde Oplossing dient te voldoen aan de basisprincipes '***Secure / Security by Design***' en '***Secure / Security by Default***'.
IBPD-3.1.8	De geleverde Oplossing dient gevoelige en/of vertrouwelijke gegevens '***in transit***' en '***at rest***' te versleutelen op basis van algemeen geaccepteerde best practices en in lijn met de adviezen van het Nationaal Cyber Security Centrum (NCSC).
IBPD-3.1.9	De geleverde Oplossing dient bij gebruik van encryptiesleutels en/of certificaten ervoor zorg te dragen dat het gebruik voor de opdrachtgever inzichtelijk is, het beheer bij de opdrachtgever kan komen te liggen en dat het per direct intrekken of onbruikbaar maken van encryptiesleutels en/of certificaten mogelijk is.
IBPB-3.1.10	Opdrachtnemer dient voor het onderhoud en/of doorvoeren van aanpassingen met betrekking tot de geleverde Oplossing een wijzigingsproces te hebben en te hanteren, waarbij de nadruk ligt op het voorkomen van beveiligingsincidenten, storingen en/of onderbrekingen tijdens het doorvoeren van veranderingen.

Eis	Omschrijving
IBPB-3.1.11	Opdrachtnemer dient Informatiebeveiliging en bedrijfscontinuïteit gestandaardiseerd, gestructureerd en gebaseerd op een cyclus van continue verbeteren in alle lagen van de organisatie en de geleverde Dienstverlening te hebben ingericht.
IBPB-3.1.12	Opdrachtnemer dient beleid, beleids- en beheersingsrichtlijnen en processen te hebben voor het veilig beheren en aanbieden van de Dienstverlening.
IBPB-3.1.13	Opdrachtnemer dient procedures te hebben, uit te voeren en over de resultaten te rapporteren met betrekking tot het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de geïmplementeerde maatregelen ter beveiliging van de geleverde Dienstverlening. Dit dient periodiek, minimaal iedere 3 jaar, en daarnaast ook altijd opnieuw bij significante wijzigingen te gebeuren.

3.2 Risicoanalyses

Risicoanalyses hebben tot doel om alle mogelijk relevante dreigingen / risico's en gevolgen in kaart te brengen. Een risico is niet direct een gevaar, maar kan dit in de toekomst wel worden. Eventueel kunnen op basis van de uitkomsten van een risicoanalyse mitigerende maatregelen worden geïmplementeerd om de kans en/of de impact van het optreden van een risico te beperken. Het geleverde dient op dit onderdeel minimaal aan de hieronder staande eisen te voldoen:

Eis	Omschrijving
IBPA-3.2.1	Opdrachtnemer dient actief mee te werken aan het inzichtelijk maken en het mitigeren van risico's welke samenhangen met de Oplossing.
IBPA-3.2.2	Opdrachtnemer dient structureel risicoanalyses uit te voeren in het bouw- en implementatietraject, bij grote onderhoudstrajecten en bij significante wijzigingen in de geleverde Oplossing / Dienstverlening.
IBPA-3.2.3	Opdrachtnemer dient aantoonbaar onderkende risico's vast te leggen voorzien van de geplande mitigerende maatregelen inclusief een verwachte implementatie / oplosdatum en actiehouder.
IBPB-3.2.4	Opdrachtnemer dient conform afspraken in de Overeenkomst te rapporteren over de status van de onderkende risico's en de bijbehorende voortgang van de geplande te implementeren mitigerende maatregelen.
IBPB-3.2.5	Opdrachtnemer dient opdrachtgever op de hoogte te stellen, via het overeengekomen communicatiekanaal en tijdslijnen, van risico's die een directe impact op de opdrachtgever (kunnen) hebben.

3.3 Logische toegangsbeveiliging

Logische toegangsbeveiliging heeft tot doel de toegang tot data / informatie, IT-voorzieningen en bedrijfsprocessen op grond van de bedrijfsbehoeften en Informatiebeveiligings- en Privacy te beheersen. Het geleverde dient op dit onderdeel minimaal aan de hieronder staande eisen te voldoen:

Eis	Omschrijving
IBPA-3.3.1	De geleverde Oplossing dient te beschikken over passende, betrouwbare en effectieve mechanismen, gebaseerd op algemeen geaccepteerde standaarden, ten aanzien van identificatie, authenticatie, autorisatie en verantwoording / controle (IAAA).
IBPD-3.3.2	De geleverde Oplossing dient aan te sluiten op de aanwezige directory service (Microsoft Active Directory (AD)) van de opdrachtgever waarbij de opdrachtgever altijd eindverantwoordelijk blijft voor het vaststellen van de gedeelde attributen.
IBPD-3.3.3	De geleverde Oplossing dient voor authenticatie Multi-factor authenticatie (MFA) en single sign-on (SSO) op basis van standaard protocollen (bv. OAUTH2, SAML, etc.) te ondersteunen.
IBPD-3.3.4	De geleverde Oplossing dient zo ingericht te zijn dat gebruikers alleen toegang hebben tot gegevens voor zover dat voor de uitoefening van hun taken noodzakelijk is (autorisatie principes '***least privilege***', '***need-to-know***', '***need-to-use***' en '***Separation of duties***') en dat toegang c.q. activiteiten altijd herleidbaar zijn tot één uniek persoon.
IBPB-3.3.5	Opdrachtnemer dient beleid en ondersteunende (beveiligings-)maatregelen te hebben geïmplementeerd om de veiligheid te kunnen garanderen van gegevens die wordt benaderd, verwerkt en/of opgeslagen in opdracht van de opdrachtgever.
IBPB-3.3.6	Opdrachtnemer dient conform afspraken in de Overeenkomst de toegangsrechten van zijn medewerkers die werkzaamheden uitvoeren ten behoeve van de geleverde Dienstverlening te controleren (SOLL / IST vergelijking) en eventuele afwijkingen onmiddellijk te corrigeren.

3.4 Security hardening

Security hardening heeft tot doel om de kwetsbaarheid van ICT-componenten te reduceren / minimaliseren en daarmee het aanvalsoppervlak te verkleinen. Het geleverde dient op dit onderdeel minimaal aan de hieronder staande eisen te voldoen:

Eis	Omschrijving
IBPD-3.4.1	Hardening met betrekking tot de geleverde Oplossing dient in geval van uiteindelijk beheer door de opdrachtgever aan te sluiten op haar beleid en processen en in alle andere gevallen minimaal plaats te vinden op basis van een onafhankelijk toetsbare internationale standaard (zoals bijvoorbeeld de CIS-benchmarks) welke tevens compliant is met de laatste versie van de BIO waaraan de opdrachtgever moet voldoen.
IBPB-3.4.2	Opdrachtnemer dient volgens een beschreven en geïmplementeerd Security hardening beleid en proces de hardening van alle ICT-component die betrokken zijn bij de geleverde Oplossing te controleren en/of uit te voeren en gepaste maatregelen te nemen op basis van geconstateerde bevindingen.
IBPB-3.4.3	Opdrachtnemer dient conform afspraken in de Overeenkomst te rapporteren over afgesproken relevante Key Performance Indicatoren (KPIs) met betrekking tot het Security hardening proces inclusief de status van de opvolging / afhandeling van geconstateerde bevindingen.

3.5 Vulnerability Management

Vulnerability Management heeft tot doel om middels scanning inzicht te krijgen in de (technische) kwetsbaarheden van de gebruikte ICT-componenten binnen de IT-infrastructuur om op basis van deze informatie mitigerende maatregelen te kunnen nemen ter beperking van de risico's. Het geleverde dient op dit onderdeel minimaal aan de hieronder staande eisen te voldoen:

Eis	Omschrijving
IBPA-3.5.1	Vulnerability Management met betrekking tot de geleverde Oplossing dient in geval van uiteindelijk beheer door de opdrachtgever aan te sluiten op haar beleid en processen en in alle andere gevallen minimaal ingericht te zijn c.q. uitgevoerd te worden op basis van een onafhankelijk toetsbare internationale standaard (zoals bijvoorbeeld voor de inrichting ISO27001 en ISAE3402 SOC2 voor opzet, bestaan en werking) welke tevens compliant is met de laatste versie van de BIO waaraan de opdrachtgever moet voldoen.
IBPB-3.5.2	Opdrachtnemer dient voor in gebruik name van een nieuwe of significante aanpassing op de Oplossing een kwetsbaarheidsscan uit te voeren en indien noodzakelijk gepaste maatregelen te nemen op basis van geconstateerde bevindingen.
IBPB-3.5.3	Opdrachtnemer dient volgens een beschreven en geïmplementeerd Vulnerability Management beleid en proces met een gepaste frequentie kwetsbaarheidsscans uit te voeren op alle ICT-componenten die betrokken zijn bij de geleverde Oplossing en indien noodzakelijk gepaste maatregelen te nemen op basis van geconstateerde bevindingen.
IBPB-3.5.4	Opdrachtnemer dient conform afspraken in de Overeenkomst te rapporteren over afgesproken relevante KPIs met betrekking tot Vulnerability Management inclusief de status van de opvolging / afhandeling van geconstateerde bevindingen.

3.6 Lifecycle en Patch Management

Lifecycle en Patch Management heeft tot doel de laatste (beveiligings-)patches en updates voor componenten in de IT-infrastructuur te verwerven, testen en uit te rollen met minimale verstoring van het productieproces. Het geleverde dient op dit onderdeel minimaal aan de hieronder staande eisen te voldoen:

Eis	Omschrijving
IBPA-3.6.1	Lifecycle en Patch Management met betrekking tot de geleverde Oplossing dient in geval van uiteindelijk beheer door de opdrachtgever aan te sluiten op haar beleid en processen en in alle andere gevallen minimaal ingericht te zijn c.q. uitgevoerd te worden op basis van een onafhankelijk toetsbare internationale standaard (zoals bijvoorbeeld voor de inrichting ISO27001 en ISAE3402 SOC2 voor opzet, bestaan en werking) welke tevens compliant is met de laatste versie van de BIO waaraan de opdrachtgever moet voldoen.
IBPB-3.6.2	Opdrachtnemer dient volgens een beschreven Patch Management beleid en proces met een gepaste frequentie (beveiligings-)patches en updates door te voeren op alle ICT-componenten die betrokken zijn bij de geleverde Oplossing.
IBPB-3.6.3	Opdrachtnemer dient ervoor te zorgen dat alle bij de Oplossing betrokken ICT-componenten voorzien zijn van de laatste (beveiligings-)patches en updates en dient indien noodzakelijk gepaste maatregelen te nemen op basis van geconstateerde bevindingen.
IBPB-3.6.4	Opdrachtnemer dient bij beschikbaarheid van een (beveiligings-)patch en updates, voorafgaand aan de implementatie, de implementatierisico's te beoordelen en de patch of update te testen op een niet productieomgeving alvorens deze in productie door te voeren.
IBPB-3.6.5	Opdrachtnemer dient indien geen (beveiligings-)patch c.q. update beschikbaar is gepaste mitigerende maatregelen te implementeren opdat het restrisico tot een acceptabel niveau wordt teruggebracht.
IBPB-3.6.6	Opdrachtnemer dient conform afspraken in de Overeenkomst te rapporteren over afgesproken relevante KPIs met betrekking tot de Lifecycle en Patch Management processen inclusief de status van de opvolging / afhandeling van geconstateerde bevindingen.

3.7 Penetratietesting

Het doel van penetratietesting (binnendringingstesten) is om te toetsen of een applicatie, component of infrastructuur kwetsbaarheden heeft en of het ook mogelijk is deze kwetsbaarheden te misbruiken. Het geleverde dient op dit onderdeel minimaal aan de hieronder staande eisen te voldoen:

Eis	Omschrijving
IBPA-3.7.1	Penetratietesting met betrekking tot de geleverde Oplossing dient in geval van uiteindelijk beheer door de opdrachtgever aan te sluiten op haar beleid en processen en in alle andere gevallen minimaal ingericht te zijn c.q. uitgevoerd te worden op basis van een onafhankelijk toetsbare internationale standaard (zoals bijvoorbeeld OWASP) welke tevens compliant is met de laatste versie van de BIO waaraan de opdrachtgever moet voldoen.
IBPA-3.7.2	Opdrachtgever heeft het recht om te allen tijde een penetratietest uit te laten voeren, door een door haar te bepalen onafhankelijke derde partij, met betrekking tot de geleverde Oplossing waar de Opdrachtnemer medewerking aan dient te verlenen.
IBPB-3.7.3	Opdrachtnemer dient volgens een beschreven Penetratietesting beleid en proces penetratietest uit te laten voeren door een externe partij op alle ICT-componenten van de geleverde Oplossing.
IBPB-3.7.4	Opdrachtnemer dient voor in gebruik name van een nieuwe dienst / ICT-component of bij een significante wijziging daarvan, maar minimaal jaarlijks, een penetratietest uit te (laten) voeren en geconstateerde relevante bevindingen te mitigeren c.q. op te lossen.
IBPB-3.7.5	Opdrachtnemer dient conform afspraken in de Overeenkomst te rapporteren over de uitgevoerde penetratietesten inclusief de status van de opvolging / afhandeling van de geconstateerde bevindingen.

3.8 Infrastructuur

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. Het geleverde dient op dit onderdeel minimaal aan de hieronder staande eisen te voldoen:

Eis	Omschrijving
IBPA-3.8.1	De geleverde Oplossing dienen op een gepaste wijze te worden beschermd tegen aanvallen op de gebieden beschikbaarheid, integriteit en vertrouwelijkheid.
IBPD-3.8.2	De geleverde Oplossing dient te voldoen aan het '***Defense in depth***' concept door de inrichting van meerdere beveiligingslagen en/of maatregelen.
IBPD-3.8.3	De geleverde Oplossing dient efficiënte, effectieve, beveiligde en knoeivrije / niet muteerbare signaleringsfuncties (registratie / logging en detectie) te hebben.
IBPD-3.8.4	De geleverde Oplossing dient audit / logbestanden minimaal 15 maanden te bewaren voor toekomstig onderzoek en toegangscontrole.
IBPD-3.8.5	De geleverde Oplossing dient alleen toegankelijk te zijn voor door de opdrachtgever geautoriseerde personen en/of partijen.

Eis	Omschrijving
IBPD-3.8.6	De geleverde Oplossing dient de mogelijkheid van afluisteren van netwerkverbindingen en/of het wijzigen van datastromen te verhinderen gebruikmakend van algemeen geaccepteerde best practices.
IBPD-3.8.7	Opdrachtnemer dient gebruik te maken van een veilige ontwikkel- en integratieomgeving ter beheersing van de ontwikkeling c.q. de aanpassing van informatiesystemen.
IBPB-3.8.8	Opdrachtnemer dient loggings- en detectie-informatie (registraties en alarmeringen) en de beveiligingsstatus van ICT-componenten actief te monitoren (bewaking en analyse) en eventuele bevindingen te rapporteren en op te volgen volgens een proces.
IBPB-3.8.9	Opdrachtnemer dient media en/of ICT-componenten gerelateerd aan de Oplossing middels een formele procedure op een veilige manier te verwijderen / af te voeren.

3.9 Cloud en/of External Service Provider (ESP)

De veiligheid van de data / informatie is van essentieel belang bij het gebruik van Oplossing die vanuit de cloud en/of door een ESP wordt aangeboden. Het is dan ook belangrijk om naast de al gestelde eisen, een aantal specifieke eisen hieromtrent op te nemen. Het geleverde dient minimaal aan de hieronder staande eisen te voldoen:

Eis	Omschrijving
IBPA-3.9.1	Opdrachtnemer dient te waarborgen dat opdrachtgever te allen tijde eigenaar blijft van de gegevens welke binnen de Oplossing wordt verwerkt en/of zijn opgeslagen.
IBPD-3.9.2	De geleverde Oplossing dient logisch en functioneel gescheiden te zijn van mogelijk andere afnemers / klanten. Dit betekent onder andere zonder afhankelijkheden in geval van onderhoud en releasewerkzaamheden en/of in geval van een technische uitwijk.
IBPD-3.9.3	De geleverde Oplossing dient voor de gebruiker en het beheer van de digitale identiteit en de toegangsrechten zo ingericht te zijn zodat transparant is waar deze wordt gehost.
IBPD-3.9.4	De geleverde Oplossing dient in het kader van dataportabiliteit voorzieningen te hebben voor het exporteren van data in een algemeen gangbaar formaat (lees XML, CSV, enz.) zoals vastgelegd in de Overeenkomst.
IBPD-3.9.5	De geleverde Oplossing dient ervoor zorg te dragen dat aangeleverde documenten tijdens het gebruik, in lijn met de retentie-policy van de opdrachtgever, altijd in het aangeleverde formaat beschikbaar blijven.
IBPD-3.9.6	De geleverde Oplossing dient elke koppeling tussen applicaties / services en ICT-componenten in te richten op basis van algemeen geaccepteerde standaarden waarbij uitwisselingen tussen verschillende security domeinen verloopt via gedefinieerde koppelpunten van de opdrachtgever.
IBPB-3.9.7	Opdrachtnemer dient op verzoek van de opdrachtgever specifieke (log)data te leveren aan de (externe) Security Operations Center (SOC) en Management Operations Center (MOC) functie van de opdrachtgever.

Eis	Omschrijving
IBPB-3.9.8	Opdrachtnemer dient voor voorspelbare beveiligingsincidenten (lees bijvoorbeeld malware-uitbraken en ((distributed) denial-of-service attacks ((D)DoS)) standaard periodiek geteste scenario's / playbooks beschikbaar te hebben welke per direct kunnen worden geactiveerd.

3.10 Webapplicaties

Het beveiligen van webapplicaties heeft tot doel om te waarborgen dat webapplicaties functioneren zoals is beoogd, ingericht zijn volgens specifieke beleidsuitgangspunten van en voldoen aan de eisen die door de opdrachtgever zijn gesteld ten aanzien van de kwaliteitsaspecten vertrouwelijkheid, integriteit, beschikbaarheid en controleerbaarheid Het geleverde dient op dit onderdeel minimaal aan de hieronder staande eisen te voldoen:

Eis	Omschrijving
IBPD-3.10.1	De geleverde Oplossing dient qua standaarden en technische specificaties te voldoen aan de standaarden zoals opgesteld door het World Wide Web Consortium (W3C), dan wel de logische opvolgers daarvan.
IBPD-3.10.2	De geleverde Oplossing dient qua (cryptografische) beveiligingsmaatregelen te voldoen aan de NCSC-beveiligingsrichtlijnen, dan wel de logische opvolger daarvan.
IBPD-3.10.3	De geleverde Oplossing dient aantoonbaar geen kwetsbaarheden / kritische beveiligingsrisico's te bevatten zoals beschreven in de meest recente OWASP top 10.
IBPA-3.10.4	Opdrachtnemer dient beleid, beleids- en beheersingsrichtlijnen en processen te hebben en te hebben geïmplementeerd voor het veilig ontwikkelen van software / (web)applicaties welke onderdeel uit maken van de geleverde Oplossing.
IBPA-3.10.5	Opdrachtnemer dient bij het ontwikkelen van (web)applicaties betrokken bij de geleverde Oplossing gebruik te maken van Secure Software Development (SSD) methodiek om de Informatiebeveiligings- en Privacy aspecten te borgen.
IBPA-3.10.6	Opdrachtnemer dient beleid, beleids- en beheersingsrichtlijnen en processen te hebben voor het veilig beheren en aanbieden van software / (web)applicaties welke onderdeel uitmaakt van de geleverde Oplossing.

4 Generieke eisen ten aanzien van Privacy (P)

De AVG beschermt de grondrechten en de fundamentele vrijheden van levende natuurlijke personen en met name hun recht op bescherming van persoonsgegevens. In dit hoofdstuk worden niet de eisen herhaald die al zijn beschreven in de voorgaande hoofdstukken. Het geleverde dient additioneel op dit onderdeel minimaal aan de hieronder staande eisen te voldoen:

Eis	Omschrijving
IBPA-4.1	De geleverde Oplossing dient gedurende de gehele looptijd van de Overeenkomst te voldoen aan van toepassing zijnde wet- en regelgeving, waaronder de AVG (Algemene Verordening Gegevensbescherming).
IBPD-4.2	De geleverde Oplossing dient op het gebied van Informatiebeveiliging en Privacy maatregelen te hebben geïmplementeerd, op basis van een aantoonbaar uitgevoerde (Data) Privacy Impact Assessment ((D)PIA), passend bij de soort persoonsgegevens die worden verwerkt en in lijn met algemeen geaccepteerde standaarden.
IBPD-4.3	De Oplossing dient te voldoen aan de basisprincipes '***Privacy by Design',*** '***Privacy by Default*', '*Data Protection by Design***', '***Data Protection by Default***' en '***Data (collection and processing) minimalization***'.
IBPD-4.4	De geleverde Oplossing dient mogelijkheden te bieden om te allen tijde te voldoen aan verzoeken in het kader van de rechten van betrokkenen.
IBPD-4.5	De geleverde Oplossing dient mogelijkheden te bieden om aan personen gerelateerde gegevenselementen die niet of niet meer noodzakelijk zijn voor (latere) verwerkingen of waarvoor geen doelbinding / rechtsgrond meer aanwezig is te verwijderen.
IBPD-4.6	De geleverde Oplossing dient mogelijkheden te bieden om aan de data gerelateerde retentie-policies zelfstandig in te regelen of in te laten regelen.
IBPA-4.7	De geleverde Oplossing dient uitsluitend persoonsgegevens te verwerken, te transporteren en op te slaan binnen de Europese Economische Ruimte (EER) zodat de uitoefening van buitenlandse wetgeving niet kan leiden tot (privacy) risico's. Dit geldt ook voor eventuele back-ups!
IBPA-4.8	De locatie van de geleverde Oplossing en de daarbij betrokken medewerkers dienen zich binnen de Europese Economische Ruimte (EER) te bevinden.
IBPA-4.9	In de geleverde Oplossing dient bij de verwerking van persoonsgegevens, zonder de uitdrukkelijke schriftelijke voorafgaande toestemming van de opdrachtgever, geen gebruik te worden gemaakt van subverwerkers.
IBPB-4.10	Opdrachtnemer dient een geïmplementeerd privacybeleid te hebben met daarin de doelstellingen, rollen en verantwoordelijkheden met betrekking tot privacy welke in overstemming zijn met van toepassing zijnde wet- en regelgeving en in lijn met algemeen geaccepteerde privacy principes.
IBPB-4.11	Voorafgaand aan in productie name van de geleverde Oplossing dient een Verwerkersovereenkomst afgesloten te zijn tussen de opdrachtgever als verwerkingsverantwoordelijke en de Opdrachtnemer als verwerker indien er persoonsgegevens worden verwerkt door de Opdrachtnemer.

Eis	Omschrijving
IBPB-4.12	Opdrachtnemer dient de van opdrachtgever ontvangen persoonsgegevens uitsluitend op basis van schriftelijke instructies van de opdrachtgever te verwerken voor doeleinden die rechtstreeks voortvloeien uit de werkzaamheden die partijen zijn overeenkomen.
IBPA-4.13	Opdrachtnemer dient bij beëindiging van de Dienstverlening de voor de opdrachtgever verwerkte persoonsgegevens te retourneren dan wel op verzoek van de opdrachtgever te vernietigen, tenzij er sprake is van een wettelijke bewaarplicht.
IBPB-4.14	Opdrachtnemer dient een proces te hebben en te hebben geïmplementeerd om datalekken onverwijld, maar uiterlijk binnen 24 uur, aan de Opdrachtnemer te melden.
IBPB-4.15	Opdrachtnemer dient opdrachtgever op verzoek te allen tijde te ondersteunen bij de uitoefening van de rechten van betrokkenen en/of de opvolging of afhandeling van datalekken.

5 Generieke eisen ten aanzien van uitvoeringsaspecten

5.1 Beveiligingsincidenten

Een security of privacy incident is iedere handeling in strijd met het vastgestelde informatiebeveiligings- en/of privacybeleid van de Opdrachtnemer, of een gebeurtenis, met (mogelijk) nadelige gevolgen voor de beschikbaarheid, integriteit en/of vertrouwelijkheid van systemen en/of data / informatie, die vallen onder de verantwoordelijkheid en/of het beheer van de Opdrachtnemer. Het geleverde dient op dit onderdeel minimaal aan de hieronder staande eisen te voldoen:

Eis	Omschrijving
IBPA-5.1.1	Alle betrokken medewerkers bij de Dienstverlening dienen een informatiebeveiligings- en/of privacy incident onmiddellijk volgens de standaard procedure te melden en in ieder geval per mail bij de Servicedesk van de opdrachtgever, op het emailadres: servicedesk@svb.nl.
IBPB-5.1.2	Opdrachtnemer dient bij een informatiebeveiligings- en/of privacy incident zo snel als mogelijk passende maatregelen te treffen om de gevolgen en de schade voor alle betrokkenen te beperken en/of te voorkomen.
IBPB-5.1.3	Opdrachtnemer dient te allen tijde volledige medewerking te verlenen bij het onderzoeken en oplossen van informatiebeveiligings- en/of privacy incidenten en stelt, indien gevraagd, alle informatie met betrekking tot het incident ter beschikking aan de opdrachtgever.

5.2 Compliance

Ter ondersteuning van de eisen die de opdrachtgever stelt aan haar Opdrachtnemer, moet gedurende de looptijd van de Overeenkomst met de Opdrachtnemer een aantal controles en/of audits uitgevoerd worden. Het geleverde dient op dit onderdeel minimaal aan de hieronder staande eisen te voldoen:

Eis	Omschrijving
IBPA-5.2.1	Opdrachtnemer dient de opdrachtgever het recht te verlenen om een onderzoek (of audit) in te stellen met betrekking tot de naleving van de Overeenkomst'. De audit wordt altijd door een onafhankelijke derde partij (auditor) uitgevoerd in samenspraak met de Opdrachtnemer.
IBPB-5.2.2	Opdrachtnemer dient gedurende de looptijd van de Overeenkomst minimaal te beschikken over een geldig ISO27001 certificaat of gelijkwaardige normering en bijbehorende recente formele audit-verklaringen die passen is bij de aard van de geleverde Dienstverlening. De audit-verklaring dient te zijn afgegeven door een onafhankelijke geaccrediteerde auditor waarmee opzet, het bestaan en de werking van een passend stelsel van beveiligings- en privacy maatregelen ten aanzien van de geleverde Dienstverlening wordt aangetoond.

5.3 Overleg & rapportage

Als onderdeel van de besturing van de door Opdrachtnemer geleverde Dienstverlening vindt regulier overleg plaats met Opdrachtnemer en levert deze periodiek rapportages op. Het geleverde dient op dit onderdeel minimaal aan de hieronder staande eisen te voldoen:

Eis	Omschrijving
IBPA-5.3.1	Opdrachtnemer dient een vaste contactpersoon aan te stellen die voor de geleverde Dienstverlening verantwoordelijk is voor zowel informatiebeveiliging als privacy.
IBPA-5.3.2	Opdrachtnemer dient in samenspraak met de opdrachtgever een overlegstructuur inclusief periodiek overleggen in te richten om minimaal de overeengekomen opgeleverde rapportages, eventuele issues en ontwikkelingen rond de geleverde Dienstverlening te bespreken.
IBPB-5.3.3	Opdrachtnemer dient conform afspraken in de Overeenkomst verantwoording af te leggen over de mate van invulling en effectiviteit van de getroffen beveiligings- en privacy maatregelen en het gerealiseerde beveiligings- & privacy niveau binnen de scope van de geleverde Dienstverlening.
IBPB-5.3.4	Opdrachtnemer dient conform afspraken in de Overeenkomst te rapporteren over de overeengekomen Key Performance en Risk Indicators (KPIs / KRIs) met betrekking tot de geleverde Dienstverlening.