# Programma van Eisen

# Informatiebeveiliging en Privacy

# Inhoudsopgave

# 1 Inleiding

In deze bijlage staan de Informatiebeveiligings- en privacy eisen met betrekking tot de 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 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 privacy beleid is een viertal informatiebeveiligings- en privacy 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 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 NEN-ISO/ IEC 27002 of opvolgers hiervan, of een gelijkwaardige normering.

## 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) en de Uitvoeringswet 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.

## 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 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 Dienstverlening een geheimhoudingsverplichting opgelegd hebben gekregen t.a.v. alle informatie die hen bekend raakt (of kan raken) t.a.v. de Dienstverlening die minstens even streng is als de geheimhoudingsverplichtingen in de Overeenkomst, en dat de medewerkers hier ook daadwerkelijk naar handelen. |
| IBP-2.3 | Opdrachtnemer draagt zorg dat alle medewerkers die participeren in de levering van de Dienstverlening een Verklaring Omtrent Gedrag (VOG), of een gelijkwaardig document, hebben die geldig is tijdens de duur van de uitvoering van de werkzaamheden. |

# 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 Dienstverlening moet aan de volgende eisen voldoen.

| *Eis* | *Omschrijving* |
|---|---|
| IBP-3.1.1 | De 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 Dienstverlening ingericht. |
| IBP-3.1.3 | De 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 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 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. De eisen die aan de Dienstverlening gesteld worden moeten ook gelden voor onderaannemers. Opdrachtnemer is te allen tijde verantwoordelijk en aansprakelijk voor de borging van de overeengekomen eisen van de 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. |

## 3.2 Risicoanalyses

De wendbaarheid van de 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 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 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 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 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 Dienstverlening moet, om het toegangsproces voor de Gebruikers 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 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 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 Dienstverlening moet aan de volgende eisen voldoen.

| *Eis* | *Omschrijving* |
|---|---|
| IBP-3.4.1 | Opdrachtnemer 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 Dienstverlening systematisch voorzien worden van de vereiste patches. Het zorgt voor het verwerven, testen en installeren van patches. De 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 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. |

## 3.6 Security hardening

Security hardening is het proces dat ervoor zorgt dat alle componenten (ICT-systemen) ingezet voor de Dienstverlening op gestandaardiseerde wijze worden ingericht en structureel beheerd waarbij de insteek is om de veiligheidsrisico's zoveel mogelijk te elimineren. De 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 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:<br>▪ Applicaties;<br>▪ Middleware en databases;<br>▪ Platformen/ infrastructuur;<br>▪ Netwerken; en<br>▪ 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 Dienstverlening kwetsbaar zijn voor inbraak. De 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 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 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. |

## 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 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 Dienstverlening moet voldoen aan de NCSC ICT-Beveiligingsrichtlijnen voor Webapplicaties dan wel de logische opvolgers daarvan. |
| 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 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). |

## 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 Dienstverlening moet aan de volgende eisen voldoen.

| *Eis* | *Omschrijving* |
|---|---|
| IBP-3.9.1 | Als onderdeel van de architectuur van de Dienstverlening moet netwerksegmentatie/ zonering conform een “defense in depth” strategie worden toegepast. |
| IBP-3.9.2 | De componenten die deel uitmaken van de 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 Dienstverlening moet alleen toegankelijk zijn via de door SVB goedgekeurde Endpoints en op de SVB goedgekeurde wijze. |

## 3.10 Cloud

De veiligheid van de SVB gegevens is van kritiek belang bij het gebruik van de 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 Dienstverlening moet aan de volgende eisen voldoen.

| *Eis* | *Omschrijving* |
|---|---|
| IBP-3.10.1 | Verwerking van (waaronder doorlopende en incidentele toegang tot) data van de SVB moet uitsluitend plaatsvinden binnen de Europese Economische Ruimte (Europese Unie, Noorwegen, Liechtenstein, IJsland). Opdrachtnemer moet passende technische en organisatorische maatregelen nemen om dit te garanderen. |
| IBP-3.10.2 | Alle koppelingen tussen applicaties (interoperabiliteit) moet op basis van open standaarden plaatsvinden en worden standaard via de SVB koppelpunten geleid. Opdrachtnemer moet alle known-incompatibilities op dit vlak op voorhand en schriftelijk meedelen aan de SVB. |
| 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 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 gebruikte encryptiesleutels voor het encrypten van de data moet binnen de Dienstverlening op elk moment in het proces per direct ingetrokken of onbruikbaar kunnen worden gemaakt. |
| IBP-3.10.6 | Opdrachtnemer moet alle SVB assets op generiek, nader te bepalen, formaat en overdrachtsmechanisme aanleveren aan de SVB. Als de SVB niet meer gebruik wil/kan maken van de Dienstverlening. Dit geldt voor alle ‘tangible’ als ook ‘non-tangible’ assets van de SVB. (niet limitatief: SVB-nummerplan, (historische) gespreksdata, SVB-specifieke configuratie-instellingen, voice-recordings, speech-to-text data, etc…) |

# 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 Dienstverlening moet aan de volgende eisen voldoen.

| *Eis* | *Omschrijving* |
|---|---|
| IBP-4.1 | De Dienstverlening en de organisatie van Opdrachtnemer moeten 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:<br>▪ Het uitvoeren van testen; en<br>▪ 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 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:<br>1. Transport van persoonsgegevens over openbare of semiopenbare dat infrastructuur (internet, e-mail, extranet etc.).<br>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:<br>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).<br>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.<br>3. Beperk zoekfunctionaliteit m.b.t. persoonsgegevens en geef alleen zoekresultaten weer na het invoeren van een aantal persoonsgegevens.<br>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 Dienstverlening moet per type informatie door SVB goedgekeurde bewaartermijnen kunnen worden ingesteld. |

# 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 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 | 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 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.<br>In geval een 'gelijkwaardig' systeem voor informatiebeveiliging wordt geleverd, dient door de Opdrachtnemer te worden toegelicht waarom het systeem gelijkwaardig is aan een gecertificeerd managementsysteem. |

## 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 Dienstverlening moet aan de volgende eisen voldoen.

| *Eis* | *Omschrijving* |
|---|---|
| IBP-5.3.1 | Opdrachtnemer stelt een vaste contactpersoon aan die voor de 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 Dienstverlening. |
| IBP-5.3.4 | Elk kwartaal moeten onderstaande rapportage-vereisten worden ingevuld (specifiek voor de Dienstverlening):<br>▪ Een overzicht van de beveiligingsincidenten (inclusief datalekken) inclusief trends, evaluaties en (root cause) analyses;<br>▪ Rapportages van risico's, kwetsbaarheden (vulnerability scan resultaten), patch management, hardening afwijkingen en voortgangsrapportages over bijbehorende remediation plannen; en<br>▪ Analyse van de logging en monitoring informatie. |
| IBP-5.3.5 | Jaarlijks moeten onderstaande rapportage-vereisten worden ingevuld (specifiek voor de Dienstverlening):<br>▪ De status, handhaving en effectiviteit van de geïmplementeerde maatregelen;<br>▪ Overzicht van afwijkingen ten opzichte van beleid of Overeenkomst; en<br>▪ 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 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. |

# 6 Additionele informatiebeveiligings-eisen

Voor de Telefonie- en Communicatiediensten gelden de volgende additionele informatiebeveiligings-eisen.

## 6.1 Additionele eisen aan de Oplossing inzake Multichannel

| *Eis* | *Omschrijving* |
|---|---|
| IBP-6.1.1 | De Opdrachtnemer borgt de integriteit en vertrouwelijkheid van de informatieoverdracht tussen de Oplossing en de functionaliteiten die hiervan gebruik maken (inclusief telefonie). Hiervoor heeft de Opdrachtnemer technische controls ingericht die aan de eisen zoals vermeld bij eis IBP-3.8.4 voldoen. |
| IBP-6.1.2 | De Opdrachtnemer borgt dat de identiteit van de bron van informatie (functionaliteit van de Oplossing) aan het klant-informatiesysteem wordt doorgegeven. |
| IBP-6.1.3 | De Opdrachtnemer zorgt dat functionaliteiten (inclusief telefonie) in de Oplossing de werking van andere functionaliteiten in de Oplossing niet verstoren. |
| IBP-6.1.4 | De Opdrachtnemer borgt dat datapaden van de Communicatiekanalen (waaronder Whatsapp, telefoon, etc.) naar de functionaliteiten in de Oplossing elkaar niet beïnvloeden. |

## 6.2 Additionele eisen de Oplossing inzake telefonie

| *Eis* | *Omschrijving* |
|---|---|
| IBP-6.2.1 | De communicatie-agents (hard- en softphones van de SVB) moeten voldoende sterk worden geauthentiseerd op de telefonie-functionaliteit. |
| IBP-6.2.2 | Het verkeer tussen de communicatie-agents (hard- en softphones van de SVB) en de telefonie-functionaliteit, dient binnen het SVB-domein versleuteld te zijn. |
| IBP-6.2.3 | Eisen aan (client-)software (bijv. softphones) die op reeds bestaande IT-componenten bij SVB wordt geïnstalleerd:<br>• Statement of integrity: software moet afkomstig zijn uit een integere bron.<br>• Software wordt volgens de internationaal erkend security hardening standaarden (zoals de CIS-benchmarks) gehardend, of moet worden geconfigureerd conform de beveiligingsrichtlijnen van de leverancier van de apparatuur (zie ook hfst. 3.6).<br>• Er dient scheiding te zijn tussen gebruik en beheer van deze software.<br>• Opdrachtnemer dient geconstateerde kwetsbaarheden in de software binnen zo kort mogelijke termijn op te lossen. |

## 6.3 Overige eisen

| *Eis* | *Omschrijving* |
|---|---|
| IBP-6.3.1 | Opdrachtnemer implementeert alleen door de SVB goedgekeurde autorisatiematrices. Deze hebben betrekking op alle vormen van toegang tot alle SVB-informatie binnen deze dienst (niet limitatief: beheer van de dienst, toegang tot opgenomen gesprekken, toegang tot gespreksdata, beperkingen in gebruik telefonie (0900, buitenland), speech-to-text, etc.). |
| IBP-6.3.2 | SVB gegevens dienen niet langer dan door de SVB aangegeven tijd bewaard te worden. Bij het beëindigen van de Overeenkomst tussen de SVB en de Opdrachtnemer dienen, na bevestiging van SVB van correcte overdracht zoals beschreven in eis IBP-3.10.6, de SVB-gegevens per direct en aantoonbaar te worden verwijderd. Dit dient te gebeuren conform internationaal geaccepteerde standaarden (zoals NIST SP 800-88 Rev 1, “Guidelines for Media Sanitization” of gelijkwaardig). |