voor het leven
Sociale Verzekeringsbank

Concept Verwerkersovereenkomst

WAN- en internetconnectiviteit en aanverwante dienstverlening

tussen

De Sociale Verzekeringsbank (SVB)

En

……

DE ONDERGETEKENDEN:

De Sociale Verzekeringsbank, rechtspersoonlijkheid bezittend krachtens artikel 3 lid 2 Wet Structuur uitvoeringsorganisatie werk en inkomen, gezeteld te Amstelveen aan de Van Heuven Goedhartlaan 1 (1181 KJ), hierin rechtsgeldig vertegenwoordigd door de heer drs. S.T. Sibma, Voorzitter Raad van Bestuur, hierna te noemen: “de SVB”,

en

[naam opdrachtnemer], gevestigd en kantoorhoudend te [plaats] aan [adres] [(postcode)], hierin rechtsgeldig vertegenwoordigd door [de heer/mevrouw] [naam], [functie], hierna te noemen ‘Opdrachtnemer’,

OVERWEGEN DAT:

a. Tussen de SVB en Opdrachtnemer is een overeenkomst gesloten met betrekking tot WAN en Internetconnectiviteit en aanverwante dienstverlening (hierna te noemen: de Overeenkomst).
b. In het kader van de uitvoering van de Overeenkomst krijgt Opdrachtnemer de beschikking over persoonsgegevens zoals bedoeld in de Algemene verordening gegevensbescherming en de Uitvoeringswet AVG, hierna te noemen ‘Persoonsgegevens’ en ‘AVG’. De AVG is in Nederland verder uitgewerkt door middel van de Uitvoeringswet AVG, waar in deze Verwerkersovereenkomst de AVG wordt genoemd wordt steeds ook de Uitvoeringswet AVG bedoeld.
c. Met betrekking tot de Persoonsgegevens is de SVB verwerkingsverantwoordelijke en is Opdrachtnemer verwerker in de zin van de AVG. Een verwerker beperkt zich tot het verwerken van Persoonsgegevens zonder zeggenschap te hebben over het doel van- en de middelen voor de verwerking van Persoonsgegevens. Hij neemt geen beslissingen over het gebruik van de gegevens, de verstrekking aan derden en andere ontvangers, de duur van de opslag van de gegevens etc..
d. Ingevolge artikel 28 lid 1 AVG rust op de SVB de verplichting om uitsluitend een beroep te doen op verwerkers die afdoende garanties bieden met betrekking tot het toepassen van passende technische en organisatorische maatregelen opdat de verwerking aan de vereisten van de AVG voldoet en de bescherming van de rechten van de betrokkene is gewaarborgd.

e. Partijen wensen hun afspraken over deze verwerking van Persoonsgegevens door Opdrachtnemer vast te leggen in deze overeenkomst als bedoeld in artikel 28 lid 3 AVG, hierna te noemen ‘Verwerkersovereenkomst’.

KOMEN OVEREEN ALS VOLGT:

1. Algemeen

1.1 Deze Verwerkersovereenkomst vormt een integraal onderdeel van de Overeenkomst.

1.2 Opdrachtnemer verplicht zich jegens de SVB tot al hetgeen waartoe een Verwerker van Persoonsgegevens verplicht is op grond van het bij- of krachtens de AVG bepaalde.

1.3 Opdrachtnemer zal 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 met elkaar zijn overeengekomen in de Overeenkomst. Het is Opdrachtnemer niet toegestaan om Persoonsgegevens te kopiëren, tenzij dit voor de uitvoering van de Overeenkomst noodzakelijk is, de Persoonsgegevens aan een andere partij ter beschikking te stellen of over te dragen, dan wel om andere handelingen met de Persoonsgegevens uit te voeren dan omschreven in deze Verwerkersovereenkomst, tenzij de SVB hiervoor uitdrukkelijke schriftelijke toestemming heeft gegeven. De diensten die door Opdrachtnemer zullen worden verricht zijn beschreven in de Overeenkomst en de daarbij behorende bijlagen. **Bijlage I** bevat een overzicht van de Persoonsgegevens die Opdrachtnemer voor de SVB verwerkt en het doel en de aard van de verwerkingen.

1.4 Indien Opdrachtnemer op grond van een Unierechtelijke of lidstaatrechtelijke bepaling verplicht is tot een bepaalde verwerking, stelt Opdrachtnemer de SVB voorafgaand aan de verwerking in kennis van dat wettelijk voorschrift, tenzij die wetgeving deze kennisgeving om gewichtige redenen van algemeen belang verbiedt. Opdrachtnemer stelt de SVB onmiddellijk in kennis indien naar de mening van Opdrachtnemer een instructie van de SVB inbreuk maakt op de AVG of op andere Unierechtelijke of lidstaatrechtelijke bepalingen inzake gegevensbescherming.

2. Beveiligingsmaatregelen

2.1 Opdrachtnemer verplicht zich passende maatregelen te nemen en te onderhouden tot technische en organisatorische beveiliging tegen onbevoegde toegang tot de Persoonsgegevens, verlies of tegen enige vorm van onrechtmatige verwerking van de Persoonsgegevens, overeenkomstig artikel 32 AVG. Deze maatregelen zullen in ieder geval betrekking hebben op:

- transport van Persoonsgegevens;
- fysieke en logische (toegangs)beveiliging tot apparatuur en systemen;
- logging, monitoring en controle op het netwerk en systemen;
- beheer(sing) van technische kwetsbaarheden en (security) patches;
- de informatiebeveiligingsbewustwording van medewerkers;

- afhandelen van beveiligingsincidenten en datalekken;
- continuïteitsbeheer en back-up/restore maatregelen;
- vernietigen van gegevens bij vervangen of afvoeren van gegevensdragers;
- een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen.

2.2 Opdrachtnemer draagt in het kader van zijn verplichtingen uit hoofde van artikel 32 AVG ten minste zorg voor voorzieningen van technische en organisatorische aard zoals volgen uit de meest actuele versie van NEN-ISO/IEC 27001.

2.3 De in artikel 2.1 bedoelde beveiligingsmaatregelen dienen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau te bieden gelet op de risico's die de verwerking en de aard van te beschermen gegevens met zich meebrengen. Deze maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van Persoonsgegevens te voorkomen. De beveiligingsmaatregelen die door Opdrachtnemer dienen te worden genomen zijn gebaseerd op een risicoanalyse, uitgevoerd door Opdrachtnemer, en dekken de risico's zodanig af dat aan de beveiligingseisen wordt voldaan. Naarmate de vereiste beschikbaarheid, integriteit en vertrouwelijkheid c.q. het vereiste beveiligingsniveau hoger is, treft Opdrachtnemer meer en zwaardere beveiligingsmaatregelen om de aanwezige risico's af te dekken en het vereiste beveiligingsniveau daadwerkelijk te garanderen.

2.4 Opdrachtnemer heeft de in artikel 2.1 bedoelde beveiligingsmaatregelen uitgewerkt in een informatiebeveiligingsplan dat als Bijlage II bij deze Verwerkersovereenkomst is bijgesloten.

2.5 Opdrachtnemer verbindt zich jegens de SVB om het niveau van zijn technische en organisatorische maatregelen te handhaven, waar mogelijk te verbeteren en te verfijnen en aan te passen aan de voortschrijdende technologische en maatschappelijke ontwikkelingen. Opdrachtnemer zal hiertoe actuele ontwikkelingen volgen en additionele voorzieningen treffen voor zover dat redelijkerwijs van hem kan worden verwacht.

2.6 Opdrachtnemer garandeert dat onbevoegd personeel geen toegang heeft tot de Persoonsgegevens en/of de gegevensverwerkende toepassingen. Opdrachtnemer verklaart dat ieder van zijn medewerkers die door Opdrachtnemer wordt gemachtigd tot toegang tot de Persoonsgegevens verplicht is tot geheimhouding van de Persoonsgegevens waarvan hij kennis neemt.

3. Inbreuken in verband met Persoonsgegevens

3.1 Opdrachtnemer meldt ieder datalek (een 'inbreuk in verband met persoonsgegevens' zoals bedoeld in artikel 4 AVG) waarbij Persoonsgegevens van de SVB zijn betrokken onverwijld, maar uiterlijk binnen 24 uur na ontdekking, aan de SVB. In **Bijlage III** is vastgelegd wanneer er sprake is van een datalek en zijn afspraken gemaakt over de inhoud en verzending van de rapportage van datalekken.

3.2 Indien Opdrachtnemer vaststelt dat sprake is van een datalek, zal hij alle noodzakelijke maatregelen treffen om verdere ontsluiting dan wel verspreiding van Persoonsgegevens te voorkomen. Opdrachtnemer zal hiertoe in overleg treden met de SVB en de aanwijzingen van de SVB direct opvolgen. Opdrachtnemer zal de SVB steeds op de hoogte houden van de ontwikkelingen met betrekking tot het datalek en de maatregelen die hij treft en heeft getroffen om de gevolgen van het datalek te beperken en herhaling van het datalek te voorkomen. Opdrachtnemer werkt op aangeven van de SVB mee aan het adequaat informeren van betrokkenen. Voor de duidelijkheid wordt opgemerkt dat de Opdrachtnemer het datalek niet zelf bij de autoriteiten of betrokkenen hoeft te melden. Daarvoor draagt de SVB zorg.

4. Sub-verwerkers en data-doorgiften

4.1 Het is Opdrachtnemer niet toegestaan bij de verwerking van Persoonsgegevens gebruik te maken van sub-verwerkers, zonder de uitdrukkelijke schriftelijke voorafgaande toestemming van de SVB. De SVB kan aan de toestemming om sub-verwerkers in te schakelen nadere voorwaarden verbinden. Opdrachtnemer garandeert dat hij aan haar sub-verwerkers dezelfde verplichtingen oplegt als opgenomen in deze Verwerkersovereenkomst. Opdrachtnemer blijft te allen tijde volledig aansprakelijk voor het nakomen van de verplichtingen in deze Verwerkersovereenkomst.

4.2 Opdrachtnemer garandeert dat geen Persoonsgegevens zullen worden verwerkt buiten de Europese Economische Ruimte (Europese Unie, Noorwegen, Liechtenstein, IJsland) en dat geen sprake is van activiteiten van Opdrachtnemer binnen de grenzen van de Verenigde Staten die onder de jurisdictie van de Verenigde Staten vallen.

4.3 In het geval de leverancier, of (één van) zijn sub-verwerkers gevestigd is in een derde land buiten de EER, toont de leverancier op voorhand aan dat sprake is van een passend beschermingsniveau.

5. Informatieplichten en bijstand

5.1 Opdrachtnemer voorziet de SVB van de noodzakelijke informatie waardoor de SVB een oordeel kan vormen over de naleving door Opdrachtnemer van de beveiligingsmaatregelen. Opdrachtnemer zal minimaal eens per jaar een gestructureerd overleg voeren met de SVB om

het om informatiebeveiliging bespreken. In dit overleg zal Opdrachtnemer o.a. aanpassingen in het plan toelichten. Opdrachtnemer levert jaarlijks een rapportage aan van een externe auditdienst waaruit blijkt dat haar informatiebeveiliging op orde is en conform deze Verwerkersovereenkomst.

5.2 Opdrachtnemer zal aan de SVB bijstand verlenen bij de afhandeling van verzoeken van betrokkenen op grond van hoofdstuk III van de AVG, onder meer door passende technische en organisatorische maatregelen te treffen. Het is de SVB toegestaan betrokkenen te informeren dat gebruik wordt gemaakt van Opdrachtnemer bij het verwerken van Persoonsgegevens. In het geval een betrokkene een verzoek op grond van hoofdstuk III van de AVG richt tot Opdrachtnemer, zal Opdrachtnemer het verzoek doorsturen aan de SVB, en zal de SVB het verzoek verder afhandelen.

5.3 Opdrachtnemer zal, rekening houdend met de aard van de verwerking en de hem ter beschikking staande informatie, aan de SVB bijstand verlenen bij het doen nakomen van de verplichtingen uit hoofde van de artikelen 32 tot en met 36 van de AVG.

6. Audit

6.1 De SVB heeft het recht om bij Opdrachtnemer een onderzoek (hierna 'Audit') in te stellen met betrekking tot de naleving van de in deze Verwerkersovereenkomst opgenomen verplichtingen, overeenkomstig artikel 28 lid 3 onder h AVG. De SVB kan de Audit zelf uitvoeren of laten uitvoeren door onafhankelijke deskundigen. Opdrachtnemer verplicht zich om in dit verband de systemen, bestanden en documentatie met betrekking tot de verwerking van de Persoonsgegevens op daartoe strekkend verzoek van de SVB beschikbaar te houden.

6.2 De SVB zal een Audit tijdig aankondigen. De SVB biedt Opdrachtnemer desgewenst de mogelijkheid de naleving van deze Verwerkersovereenkomst aan te tonen langs andere weg dan de door of in opdracht van de SVB uitgevoerde Audit, bijvoorbeeld door het aanleveren van een recent auditrapport van een erkende en onafhankelijke auditor, onverminderd het auditrecht dat de SVB heeft zoals bedoeld in artikel 28 lid 3 onder h AVG.

6.3 Indien Opdrachtnemer in verband met geheimhoudingsverplichtingen richting andere klanten geen inzage mag geven in bepaalde gegevens of systemen, dan zal Opdrachtnemer dit voorafgaand aan de Audit aan de SVB kenbaar maken. Zolang deze beperkingen er in redelijkheid niet aan in de weg staan om de nakoming van de Verwerkersovereenkomst te controleren, zal de SVB met deze beperkingen instemmen.

6.4 Indien de Audit aantoont dat Opdrachtnemer op een of meer punten tekortschiet in de naleving van deze Verwerkersovereenkomst, zal Opdrachtnemer vervolgens aan de SVB een voorstel doen

ten aanzien van de randvoorwaarden en uitgangspunten van de Audit, waarna Partijen in gezamenlijk overleg afspraken maken over de nadere invulling van de Audit. Opdrachtnemer zal daarbij alle redelijkerwijze te treffen maatregelen nemen om te zorgen dat hij hier alsnog aan voldoet. De kosten van de Audit en eventuele noodzakelijke aanpassingen die hieruit voortvloeien zijn voor Opdrachtnemer.

7. Verplichtingen bij einde Overeenkomst

7.1 Opdrachtnemer verplicht zich de Persoonsgegevens niet langer te bewaren dan noodzakelijk is voor uitvoering van de Overeenkomst met de SVB, en deze, inclusief alle door de SVB ter hand gestelde gegevens, documenten, bescheiden en andere goederen waaronder gegevens en informatiedragers onverwijld te retourneren dan wel op verzoek van de SVB passend te vernietigen na beëindiging van de Overeenkomst met de SVB of zoveel eerder of later als de SVB daarom uitdrukkelijk verzoekt, tenzij opslag van de Persoonsgegevens wettelijk is verplicht. Opdrachtnemer is gehouden digitale (Persoons)gegevens in een open bestandsformaat aan de SVB te retourneren. Dit geldt eveneens voor de Persoonsgegevens welke zich eventueel op grond van artikel 4.1 bevinden bij een zogenaamde sub-verwerker.

7.2 Indien een wijziging in de verwerkte Persoonsgegevens of in de beveiligingseisen daar aanleiding toe geeft, is de SVB bevoegd heronderhandelingen te voeren over een of meerdere bepalingen van deze Verwerkersovereenkomst, een onafhankelijke audit te laten uitvoeren dan wel, indien de aard van de wijziging daar aanleiding toe geeft, de Verwerkersovereenkomst tussentijds te beëindigen.

8. Boeteclausule

8.1 Opdrachtnemer is zich bewust van wettelijke en maatschappelijke taken en verantwoordelijkheden van de SVB, met name ook in relatie tot de door de SVB verwerkte persoonsgegevens. De opgedragen verwerkingen in het onderhavige geval nopen tot grote zorgvuldigheid. Om het belang daarvan te benadrukken komen partijen overeen dat Opdrachtnemer aan de SVB een direct opeisbare boete verbeurt indien Opdrachtnemer toerekenbaar tekortschiet in de nakoming van deze Verwerkersovereenkomst, onverminderd de overige rechten van de SVB. De boete bedraagt € 25.000,- per overtreding, en € 2.500,- voor ieder(e) (gedeelte van een) dag dat deze overtreding voortduurt. Zulks laat onverlet het recht van de SVB om volledige schadevergoeding van Opdrachtnemer te vorderen.

8.2 Opdrachtnemer is, in geval van zijn tekortschieten in de nakoming van deze verwerkersovereenkomst, aansprakelijk voor de schade die de SVB leidt in verband met

aanspraken van derden, ongeacht of deze derden zich richten tot Opdrachtnemer dan wel tot de SVB. Onder aanspraken van derden zijn in ieder geval (ook) begrepen aanspraken van betrokkene(n) en de door de toezichthoudende autoriteit opgelegde boetes. Op het voorgaande zijn geen beperkingen of uitsluitingen van aansprakelijkheid van toepassing, tenzij uitdrukkelijk in deze Verwerkersovereenkomst bepaald.

9. Slotbepaling

9.1 Op deze Verwerkersovereenkomst is Nederlands recht van toepassing. Alle geschillen voortvloeiende uit deze Verwerkersovereenkomst zijn uitsluitend onderworpen aan het oordeel van de bevoegde rechter te Amsterdam.

Aldus overeengekomen en in tweevoud getekend.

Amstelveen, [datum]	[plaats], [datum]
Sociale Verzekeringsbank	[naam Opdrachtnemer]
[naam]	[naam]
[functie]	[functie]

Bijlage I – Overzicht Persoonsgegevens

Onderwerp/aard en doel van de verwerking	Opdrachtnemer verricht de navolgende verwerkingen met deze Persoonsgegevens, voor de navolgende doelen: [Doel en aard verwerkingen beschrijven]
Soorten Persoonsgegevens die Opdrachtnemer verwerkt	Opdrachtnemer verwerkt in opdracht van de SVB de navolgende soorten Persoonsgegevens: [VERWIJDEREN WAT NIET VAN TOEPASSING IS EN EVT. AANVULLEN] a. Naam-, adres- en woonplaatsgegevens b. Telefoonnummers c. E-mailadressen, IP-adressen of andere adressen voor elektronische communicatie d. Toegangs- of identificatiegegevens (bijvoorbeeld inloggegevens, wachtwoorden, klantnummers) e. Financiële gegevens (bijvoorbeeld rekeningnummers, creditcardnummers, opgebouwde pensioenrechten) f. Burgerservicenummers (BSN) of sofinummers g. Paspoortkopieën of kopieën van andere legitimatiebewijzen h. Geslacht, geboortedatum en/of leeftijd i. Bijzondere Persoonsgegevens (bijvoorbeeld ras, etniciteit, criminele gegevens, politieke overtuiging, vakbondslidmaatschap, religie, seksuele leven, medische gegevens) j. Overige gegevens, namelijk: …
Categorieën van betrokkenen waarop de Persoonsgegevens betrekking hebben	Deze Persoonsgegevens hebben betrekking op de navolgende categorieën van betrokkenen: [VERWIJDEREN WAT NIET VAN TOEPASSING IS EN EVT. AANVULLEN] a. Klanten van de SVB b. Personeel van de SVB (in dienst) c. Inhuurkrachten van de SVB (niet in dienst)

	d. Sollicitanten van de SVB e. Zakelijke relaties van de SVB f. Overige betrokkenen, namelijk: …

Bijlage II – Beveiligingsplan Opdrachtnemer

[Beveiligingsplan]

[*Statement of compliance (inclusief statement of applicability)*]

[Auditverklaring]

Bijlage III – Meldplicht Datalekken

Een datalek (‘een inbreuk in verband met persoonsgegevens’) wordt in de AVG gedefinieerd als "een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens" (artikel 4 sub 12 AVG).

Een datalek is een veiligheidsincident, daarbij zijn Persoonsgegevens dus blootgesteld aan datgene waartegen de beveiligingsmaatregelen bescherming moeten bieden. De inbreuk heeft altijd betrekking op een of meerdere van de volgende informatiebeveiligingsprincipes: vertrouwelijkheid, integriteit en/of beschikbaarheid. Het begrip datalek moet ruim worden uitgelegd, zodat ook een tijdelijke inbreuk daaronder valt.

Voor de vraag of al dan niet sprake is van een datalek, is het niet van belang of de verwerkingsverantwoordelijke of verwerker passende technische of organisatorische beschermingsmaatregelen heeft getroffen. Wel kunnen deze maatregelen van belang zijn voor de verplichting het datalek te melden bij de AP en/of betrokkenen. Indien bijvoorbeeld de bij het datalek betrokken Persoonsgegevens onbegrijpelijk of ontoegankelijk zijn gemaakt voor eenieder die geen recht heeft op kennisname van de gegevens, dan is het niet waarschijnlijk dat dit een risico inhoudt voor de rechten en vrijheden van natuurlijke personen, en hoeft het datalek in beginsel niet te worden gemeld bij de AP en/of betrokkenen. Het datalek zal ook in een dergelijk geval wel door Opdrachtnemer aan de SVB gemeld moeten worden, zodat de SVB de meldingsplicht per datalek kan beoordelen.

De AP benoemt enkele voorbeelden van datalekken:

- een kwijtgeraakte USB-stick met Persoonsgegevens;
- een gestolen laptop met Persoonsgegevens;
- een inbraak door een hacker;
- verzending van e-mail waarin de e-mailadressen van alle geadresseerden zichtbaar zijn voor alle andere geadresseerden;
- een malware-besmetting;
- een calamiteit zoals een brand in een datacentrum.

Opdrachtnemer is gehouden ieder datalek onverwijld, maar uiterlijk binnen 24 uur na ontdekking, aan de SVB te melden.

Opdrachtnemer is gehouden de SVB op de hoogte te brengen van een mogelijk datalek door middel van een melding aan:

Servicedesk SVB (servicedesk@svb.nl)

Opdrachtnemer zal in haar melding aan de SVB – voor zover mogelijk – in ieder geval de volgende gegevens verstrekken (let op: vermeld in de initiële melding van het incident geen Persoonsgegevens):

1. **Een samenvatting van het incident waarbij de inbreuk op de beveiliging van Persoonsgegevens zich heeft voorgedaan.**

2. **Van hoeveel personen zijn Persoonsgegevens betrokken bij de inbreuk?**
   Minimaal: ……
   Maximaal: ……..

3. **Omschrijf de groep mensen van wie persoonsgegevens zijn betrokken bij de inbreuk.**

4. **Wanneer vond de inbreuk plaats? (Kies een van de volgende opties en vul waar nodig aan)**
   Op de volgende datum:
   Tussen de volgende data:
   Nog niet bekend

5. **Wat is de aard van de inbreuk? (Meerdere opties mogelijk)**

a. Persoonsgegevens zijn gelezen door personen die hiertoe geen recht hadden
b. Persoonsgegevens zijn gekopieerd door personen die hiertoe geen recht hadden
c. Persoonsgegevens zijn veranderd door personen die hiertoe geen recht hadden
d. Persoonsgegevens zijn verwijderd of vernietigd
e. Persoonsgegevens zijn gestolen
f. Nog niet bekend

6. Om welk type persoonsgegevens gaat het? (Meerdere opties mogelijk)

a. Naam-, adres- en woonplaatsgegevens
b. Telefoonnummers
c. E-mailadressen, IP-adressen of andere adressen voor elektronische communicatie
d. Toegangs- of identificatiegegevens (bijvoorbeeld inloggegevens, wachtwoorden, klantnummers)
e. Financiële gegevens (bijvoorbeeld rekeningnummers, creditcardnummers)
f. Burgerservicenummers (BSN) of sofinummers
g. Paspoortkopieën of kopieën van andere legitimatiebewijzen
h. Geslacht, geboortedatum en/of leeftijd
i. Bijzondere Persoonsgegevens (bijvoorbeeld ras, etniciteit, criminele gegevens, politieke overtuiging, vakbondslidmaatschap, religie, seksuele leven, medische gegevens)
j. Overige gegevens, namelijk: ….

7. Zijn de persoonsgegevens versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk gemaakt voor onbevoegden? (Kies een van de volgende opties en vul waar nodig aan)

Ja

Nee

Deels, namelijk: ….

8. Als de persoonsgegevens geheel of deels onbegrijpelijk of ontoegankelijk zijn gemaakt, op welke manier is dit dan gebeurd? Als gebruik is gemaakt van encryptie, licht dan ook de wijze van versleutelen toe.

9. Welke gevolgen kan de inbreuk hebben voor de persoonlijke levenssfeer van de betrokkenen? (Meerdere opties mogelijk)

a. Stigmatisering of uitsluiting
b. Schade aan de gezondheid
c. Blootstelling aan (identiteits)fraude
d. Blootstelling aan spam of phishing
e. Anders, namelijk: ….

10. **Welke technische en organisatorische maatregelen heeft de Verwerker reeds getroffen of zal Verwerker treffen om de nadelige gevolgen van de inbreuk te beperken en om inbreuken in de toekomst te voorkomen?**

11. **Heeft de inbreuk betrekking op personen in andere EU-landen?**

    Ja

    Nee

    Nog niet bekend

12. **Welke persoon kan nadere informatie verstrekken over het datalek?**

    Naam:

    Functie:

    E-mailadres:

    Telefoonnummer:

De SVB-functionaris zal na ontvangst van de informatie de verder te volgen stappen met Opdrachtnemer bespreken.