

BIJLAGE M – VERWERKERSOVEREENKOMST

Europese aanbesteding voor Vervanging MijnHR

VERWERKERSOVEREENKOMST

DE ONDERGETEKENDEN:

1. **Sociale verzekeringsbank**, rechtspersoonlijkheid bezittend krachtens artikel 3 lid 2 Wet Structuur uitvoeringsorganisatie werk en inkomen, gevestigd en kantoorhoudend te Amstelveen aan de Van Heuven Goedhartlaan 1 (1181 KJ), hierin rechtsgeldig vertegenwoordigd door [de heer/mevrouw] [naam], [functie], hierna te noemen te noemen **SVB**,

en

2. [naam Verwerker], gevestigd en kantoorhoudend te [plaats] aan [adres] [(postcode)], hierin rechtsgeldig vertegenwoordigd door [de heer/mevrouw] [naam], [functie], hierna te noemen **Verwerker**,

hierna ook afzonderlijk te noemen **Partij**, of gezamenlijk te noemen **Partijen**,

OVERWEGENDE DAT:

- (A) SVB (Verwerkingsverantwoordelijke) en Verwerker op [datum] een overeenkomst hebben gesloten met betrekking tot Vervanging MijnHR, (de **Overeenkomst**);
- (B) In het kader van de uitvoering van de Overeenkomst verleent Verwerker diensten aan SVB;
- (C) Verwerker in het kader de uitvoering van de Overeenkomst ook Persoonsgegevens verwerkt voor SVB;
- (D) Partijen op grond van artikel 28 lid 1 van de AVG verplicht zijn afspraken te maken en vast te leggen met betrekking tot de Verwerking van Persoonsgegevens door Verwerker;
- (E) Partijen in deze Verwerkersovereenkomst hun afspraken over het verwerken van de Persoonsgegevens door Verwerker wensen vast te leggen.

KOMEN OVEREEN ALS VOLGT:

1. DEFINITIES

- 1.1. In deze Verwerkersovereenkomst worden de navolgende gedefinieerde begrippen met een begin hoofdletter gebruikt:

AP: de Autoriteit Persoonsgegevens, de toezichthoudende autoriteit voor de naleving van de geldende Gegevensbeschermingswetgeving.

AVG: Algemene Verordening Gegevensbescherming, voluit: Verordening (EU) 2016/679 van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de Verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG.

Bijlage: iedere bijlage bij deze Verwerkersovereenkomst, die een onlosmakelijk deel daarvan uitmaakt.

Datalek: een "inbreuk in verband met persoonsgegevens" in de zin van art. 4 lid 12 van de AVG.

EER: Europese Economische Ruimte (Europese Unie, Noorwegen, Liechtenstein, IJsland).

Gegevensbeschermingswetgeving: alle toepasselijke wet- en regelgeving met betrekking tot de Verwerking en bescherming van persoonsgegevens, waaronder maar niet beperkt tot de AVG en de Uitvoeringswet Algemene Verordening Gegevensbescherming (**UAVG**).

Subverwerker: elke derde partij die door Verwerker is aangesteld om Persoonsgegevens te Verwerken.

Verwerkersovereenkomst: deze Verwerkersovereenkomst inclusief alle bijlagen die onlosmakelijk hieraan zijn verbonden.

De termen **Verwerkingsverantwoordelijke**, **Verwerker**, **Betrokkene**, **Lidstaat**, **Persoonsgegevens**, en **Verwerking** hebben dezelfde betekenis als in de AVG.

2. VERWERKING VAN PERSOONSGEGEVENS

- 2.1. Verwerker verwerkt de Persoonsgegevens uitsluitend in opdracht van SVB in het kader van de uitvoering van de Overeenkomst op basis van de schriftelijke instructies van SVB en in overeenstemming met de Gegevensbeschermingswetgeving.
- 2.2. Verwerker verwerkt de Persoonsgegevens niet voor andere doeleinden of op andere wijze dan het doel waarvoor de Persoonsgegevens zijn verstrekt of haar bekend zijn geworden.
- 2.3. De categorieën van Betrokkenen, het soort Persoonsgegevens, de aard en het doel waarvoor de Persoonsgegevens worden verwerkt, zijn vermeld in Bijlage 1.
- 2.4. Verwerker zal de Persoonsgegevens niet aan een derde verstrekken, tenzij die verstrekking plaatsvindt in opdracht van SVB, in het kader van de uitvoering van de Overeenkomst of wanneer dit noodzakelijk is om te voldoen aan een wettelijke verplichting.
- 2.5. Verwerker zal de Persoonsgegevens uitsluitend aan die medewerkers ter beschikking stellen die de Persoonsgegevens nodig hebben voor de uitvoering van hun werkzaamheden c.q. noodzakelijkerwijs van de Persoonsgegevens kennis dienen te nemen in het kader van en ter uitvoering van de Overeenkomst, en voor het overige geheimhouden, behoudens op haar rustende afwijkende wettelijke verplichtingen.
- 2.6. Partijen verstrekken elkaar over en weer tijdig alle benodigde informatie voor de Verwerking van Persoonsgegeven en voor de naleving van de Gegevensbeschermingswetgeving.
- 2.7. Deze Verwerkersovereenkomst vormt een integraal onderdeel van de Overeenkomst en vervangt, indien van toepassing, eerder gemaakte (mondelinge en schriftelijke) afspraken tussen SVB en Verwerker ter zake van de Verwerking van Persoonsgegevens.
- 2.8. In geval van tegenstrijdigheid tussen de bepalingen uit deze Verwerkersovereenkomst, de bepalingen uit de Overeenkomst en/of eerdere gemaakte afspraken, prevaleren de bepalingen uit deze Verwerkersovereenkomst, tenzij in deze Verwerkersovereenkomst uitdrukkelijk anders is bepaald.
- 2.9. Indien Verwerker op grond van een Unierechtelijke of lidstaatrechtelijke bepaling verplicht is tot een bepaalde Verwerking, stelt Verwerker SVB voorafgaand aan die Verwerking in kennis van dat wettelijk voorschrift, tenzij die wetgeving deze kennisgeving om gewichtige redenen van algemeen belang verbiedt. Verwerker stelt SVB onmiddellijk in kennis indien naar de mening van Verwerker een instructie van SVB inbreuk maakt op de Gegevensbeschermingswetgeving.

3. SUBVERWERKERS

- 3.1. Het is Verwerker niet toegestaan bij de Verwerking van Persoonsgegevens gebruik te maken van Subverwerkers, zonder de uitdrukkelijke schriftelijke voorafgaande toestemming van SVB. SVB kan aan de toestemming om Subverwerkers in te schakelen nadere voorwaarden verbinden. Verwerker zal een schriftelijke overeenkomst met die Subverwerker afsluiten en daarbij de Subverwerker dezelfde verplichtingen opleggen als die op Verwerker zelf rusten uit hoofde van deze Verwerkersovereenkomst. Verder zal Verwerker in die overeenkomst de Subverwerker verbieden derden in te schakelen. Verwerker blijft te allen tijde volledig aansprakelijk voor het nakomen van de verplichtingen in deze Verwerkersovereenkomst.
- 3.2. Verwerker houdt een actueel register bij van de door haar ingeschakelde Subverwerkers of derden waarin onder meer de identiteit, de vestigingsplaats en een beschrijving van de werkzaamheden van de Subverwerkers of derden zijn vermeld alsmede eventuele door Verwerkingsverantwoordelijke gestelde aanvullende voorwaarden.
- 3.3. Verwerker garandeert dat geen Persoonsgegevens zullen worden verwerkt buiten de EER. Persoonsgegevens mogen enkel worden verwerkt buiten de EER indien sprake is van een passend beschermingsniveau, in overeenstemming wordt gehandeld met de artikelen 44 tot en met 49 AVG en SVB hiervoor specifieke schriftelijke voorafgaande toestemming heeft verleend.

4. GEHEIMHOUDING

- 4.1. Verwerker houdt de Persoonsgegevens die zij verwerkt in het kader van de uitvoering van de Overeenkomst geheim en zal alle nodige maatregelen treffen om geheimhouding van de Persoonsgegevens te verzekeren. Verwerker zal de verplichting tot geheimhouding tevens opleggen aan haar personeel en alle eventueel door haar ingeschakelde personen.
- 4.2. De in dit artikel bedoelde geheimhoudingsplicht geldt niet indien SVB uitdrukkelijk schriftelijk toestemming heeft gegeven om de Persoonsgegevens aan een derde te verstrekken, of een wettelijke verplichting bestaat om de Persoonsgegevens aan een derde te verstrekken.

5. BEVEILIGING PERSOONSGEGEVENS

- 5.1. Verwerker zal in overeenstemming met de Gegevensbeschermingswetgeving passende technische en organisatorische beveiligingsmaatregelen treffen, in stand houden en zo nodig aanpassen om een op het risico afgestemd beveiligingsniveau te waarborgen. De maatregelen zijn er mede op gericht verlies of enige vorm van onzorgvuldige, onrechtmatige of ongeoorloofde Verwerking en Datalekken te voorkomen.
- 5.2. Verwerker heeft de in het vorige lid bedoelde beveiligingsmaatregelen uiterlijk 3 maanden na ondertekening uitgewerkt in een informatiebeveiligingsplan dat aan Bijlage 2 bij deze Verwerkersovereenkomst wordt bijgesloten.
- 5.3. Verwerker verbindt zich jegens 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. Verwerker zal hiertoe actuele ontwikkelingen volgen en additionele voorzieningen treffen voor zover dat redelijkerwijs van hem kan worden verwacht.

6. DATALEKKEN

- 6.1. Verwerker meldt ieder Datalek waarbij Persoonsgegevens van SVB zijn betrokken onverwijld, maar uiterlijk binnen 24 uur na ontdekking, aan SVB. In Bijlage 3 is vastgelegd wanneer sprake is van een Datalek en zijn afspraken gemaakt over de inhoud en verzending van de rapportage van Datalekken.

- 6.2. Indien Verwerker vaststelt dat sprake is van een Datalek, zal hij alle noodzakelijke maatregelen treffen om verdere ontsluiting dan wel verspreiding van Persoonsgegevens te voorkomen. Verwerker zal hiertoe in overleg treden met SVB en de aanwijzingen van SVB direct opvolgen. Verwerker zal 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. Verwerker werkt op aangeven van SVB mee aan het adequaat informeren van betrokkenen. Voor de duidelijkheid wordt opgemerkt dat de Verwerker het Datalek niet zelf bij de autoriteiten of Betrokkenen hoeft te melden. Daarvoor draagt de SVB zorg.

7. INFORMATIEPLICHTEN EN BIJSTAND

- 7.1. Verwerker voorziet SVB van de noodzakelijke informatie waardoor SVB een oordeel kan vormen over de naleving door Verwerker van de beveiligingsmaatregelen. Verwerker rapporteert ieder kwartaal aan SVB over de genomen maatregelen en getroffen procedures.
- 7.2. Verwerker zal aan 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. SVB zal Betrokkenen informeren dat gebruik wordt gemaakt van Verwerker bij het verwerken van Persoonsgegevens. In het geval een Betrokkene een verzoek op grond van hoofdstuk III van de AVG richt tot Verwerker, zal Verwerker het verzoek doorsturen aan SVB, en zal SVB het verzoek verder afhandelen.
- 7.3. Verwerker zal, rekening houdend met de aard van de Verwerking en de hem ter beschikking staande informatie, aan SVB bijstand verlenen bij het doen nakomen van de verplichtingen uit hoofde van de artikelen 32 tot en met 36 van de AVG.

8. AUDIT

- 8.1. SVB heeft het recht om bij Verwerker een onderzoek (**Audit**) in te stellen met betrekking tot de naleving van de in deze Verwerkersovereenkomst opgenomen verplichtingen, overeenkomstig artikel 28 lid 3 onder h AVG. SVB kan de Audit zelf uitvoeren of laten uitvoeren door onafhankelijke deskundigen. Verwerker 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.
- 8.2. SVB zal een Audit tijdig aankondigen. SVB biedt Verwerker desgewenst de mogelijkheid de naleving van deze Verwerkersovereenkomst aan te tonen langs andere weg dan de door of in opdracht van SVB uitgevoerde Audit, bijvoorbeeld door het aanleveren van een recent auditrapport van een erkende en onafhankelijke auditor onverminderd het auditrecht dat SVB heeft zoals bedoeld in artikel 28 lid 3 onder h AVG.
- 8.3. Indien Verwerker in verband met geheimhoudingsverplichtingen richting andere klanten geen inzage mag geven in bepaalde gegevens of systemen, dan zal Verwerker dit voorafgaand aan de Audit aan SVB kenbaar maken. Zolang deze beperkingen er in redelijkheid niet aan in de weg staan om de nakoming van de Verwerkersovereenkomst te controleren, zal SVB met deze beperkingen instemmen.
- 8.4. Indien de Audit aantoont dat Verwerker op een of meer punten tekortschiet in de naleving van deze Verwerkersovereenkomst, zal Verwerker vervolgens aan SVB een voorstel doen om de geconstateerde tekortkomingen te verhelpen, waarna Partijen in gezamenlijk overleg afspraken maken over de aanpassingen. De kosten van de Audit en eventuele noodzakelijke aanpassingen die hieruit voortvloeien zijn voor Verwerker.

- 8.5. In geval van een onderzoek door de Autoriteit Persoonsgegevens of een andere bevoegde autoriteit zal Verwerker alle redelijke medewerking verlenen en SVB zo spoedig mogelijk informeren.

9. AANSPRAKELIJKHEID

- 9.1. Verwerker is aansprakelijk voor alle schade voortvloeiende uit of verband houdend met het niet-nakomen van deze Verwerkersovereenkomst dan wel handelen in strijd met de Gegevensbeschermingswetgeving.
- 9.2. Verwerker vrijwaart SVB tegen aanspraken of opgelegde boetes van derden, waaronder Betrokkenen en toezichthouders, in verband met het tekortschieten van Verwerker in de nakoming van deze Verwerkersovereenkomst of overtreding door Verwerker van de Gegevensbeschermingswetgeving en zal alle daarmee verband houdende en daaruit voortvloeiende kosten (waaronder mede begrepen kosten van juridische bijstand) en schade van SVB vergoeden.

10. DUUR EN EINDE / BEWAARTERMIJN

- 10.1. Deze Verwerkersovereenkomst treedt in werking op de datum van ondertekening en eindigt van rechtswege bij beëindiging van de Overeenkomst. Verplichtingen die naar hun aard bestemd zijn om ook na beëindiging van deze Verwerkersovereenkomst voort te duren, blijven na beëindiging bestaan. Tot deze verplichtingen behoren onder meer: geheimhouding, aansprakelijkheid, toepasselijk recht en bevoegde rechter.
- 10.2. Verwerker verplicht zich de Persoonsgegevens niet langer te bewaren dan noodzakelijk is voor uitvoering van de Overeenkomst met de SVB, en deze, inclusief alle door SVB ter hand gestelde gegevens, documenten, bescheiden en andere goederen waaronder gegevens en informatiedragers onverwijld te retourneren dan wel op verzoek van SVB passend te vernietigen na beëindiging van de Overeenkomst met SVB of zoveel eerder of later als SVB daarom uitdrukkelijk verzoekt, tenzij opslag van de Persoonsgegevens wettelijk is verplicht. Verwerker is gehouden digitale (Persoons)gegevens in een open bestandsformaat aan SVB te retourneren. Dit geldt eveneens voor de Persoonsgegevens welke zich eventueel op grond van artikel 3.1 bevinden bij een zogenaamde Subverwerker.

11. WIJZIGING / TUSSENTIJDSE BEËINDIGING VERWERKERSOVEREENKOMST

- 11.1. Indien een wijziging in de verwerkte Persoonsgegevens of in de beveiligingseisen daar aanleiding toe geeft, is 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.
- 11.2. Bij wijzigingen in de werkzaamheden van Verwerker, Gegevensbeschermingswetgeving of andere relevante omstandigheden die van invloed zijn op de Verwerking van de Persoonsgegevens, treden Partijen in overleg over een eventueel benodigde wijziging van deze Verwerkersovereenkomst. Wijzigingen van deze Verwerkersovereenkomst kunnen uitsluitend schriftelijk door de bevoegde vertegenwoordigers van Partijen worden overeengekomen.

12. SLOTBEPALINGEN

- 12.1. 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.
- 12.2. Indien de Verwerkersovereenkomst strijdig is met de Overeenkomst prevaleert de Verwerkersovereenkomst.

Bijlage 1 – Te verwerken persoonsgegevens

Deze bijlage 1 bij de Verwerkersovereenkomst bevat details over de Verwerking van Persoonsgegevens.

Onderwerp/aard en doel van de Verwerking	Verwerker verricht de navolgende verwerkingen met deze Persoonsgegevens, voor de navolgende doelen: Het doel is het vastleggen van de personeelsadministratie, het verwerken van mutaties in dossiers en het leveren van data aan doelpakketten zodat de personeelsprocessen efficiënt, georganiseerd en in overeenstemming met de wet worden uitgevoerd.
Soorten Persoonsgegevens die Verwerker verwerkt	Opdrachtnemer verwerkt in opdracht van SVB de navolgende soorten Persoonsgegevens: 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. Nationaliteit j. VOG k. Arbeidsovereenkomst, aanstellingsbrief, arbeidsvoorwaardenformulier, bij doorstroom benoemingsbrief/overplaatsing l. Functie, afdeling m. Eerste en laatste werkdag n. O&R o. Klachten, waarschuwingen p. Opleiding en werkervaring q. Competenties en vaardigheden r. Oordeel m.b.t. sollicitaties s. Assessmentrapportages en testscores t. CV en motivatiebrief u. Getuigschriften en referenties

	v. NOK (contract tussen medewerker, SVB en de broker m.b.t. inhuurkrachten) w. Overige gegevens, namelijk: Studie/onderwijs, Vakantieperiode/beschikbaarheid, uitkeringsrechten, relaties, woon- en leefsituatie, werk- en uitkeringssituatie, Bestuursrechtelijke procedures, Metadata dossierbehandelingen, onderhanden zijnde werk en resultaten van afgedane werk, x. Bijzondere Persoonsgegevens, namelijk, vakbondslidmaatschap, seksuele gerichtheid¹, gezondheidsgegevens
Categorieën van betrokkenen waarop de Persoonsgegevens betrekking hebben	Deze Persoonsgegevens hebben betrekking op de navolgende categorieën van betrokkenen: a. Personeel van SVB (in dienst) b. Inhuurkrachten van SVB (niet in dienst) c. Sollicitanten van SVB d. stagiairs e. Overige betrokkenen, namelijk: sollicitanten en medewerkers met een doelgroep-indicatie
Verwerking buiten de EER	[De Persoonsgegevens worden niet buiten de EER verwerkt.] [De Persoonsgegevens worden in de volgende landen buiten de EER verwerkt (denk ook aan onderhoud door personen die zich buiten de EER bevinden of cloudopslag bij een cloudprovider van buiten de EER, zoals uit de VS): [indien van toepassing een opsomming van landen waar de Verwerking plaatsvindt/plaats kan vinden en de maatregelen die zijn getroffen om te voldoen aan de geldende wetgeving met betrekking tot de doorgifte van persoonsgegevens]
Gegevens Subverwerkers	[Niet van toepassing want niet toegestaan.] [Verwerker maakt voor de Diensten gebruik van de volgende Subverwerkers: <i>gegevens van de Subverwerkers invullen en een kopie van de overeenkomsten met de Subverwerkers bijvoegen].</i>
Contactgegevens	Mededelingen, vragen of opmerkingen in het kader van deze Verwerkingsovereenkomst zullen door Partijen worden gedaan aan onderstaande (contact)personen: Sociale Verzekeringsbank: [naam, functie en overige contactgegevens van contactpersoon, Servicedesk.svb@svb.nl]

¹ Burgerlijke staat wordt afgeleid uit de gegevens geregistreerd in het personeelssysteem. In het personeelssysteem kan de medewerker aangeven wie zijn/haar ICE (in case of emergency) contactpersoon is. Daar staat een (niet verplicht) veld waarin gevraagd wordt naar (1) de relatie van de ICE contactpersoon tot de medewerker en (2) het geslacht van de ICE-contactpersoon. De combinatie van de burgerlijke staat met deze gegevens kan iets zeggen over de seksuele gerichtheid van de medewerker.

	Verwerker: [naam, functie en overige contactgegevens van contactpersoon]
--	--

Bijlage 2 – Beveiligingsmaatregelen en plan

In deze bijlage 2 bij de Verwerkersovereenkomst zijn de afspraken tussen Partijen vastgelegd over de concrete technische en organisatorische beveiligingsmaatregelen die door de Verwerker zijn geïmplementeerd en worden onderhouden. De getroffen maatregelen kunnen worden aangevuld of gewijzigd indien dat nodig is.

De technische en organisatorische beveiligingsmaatregelen zullen in ieder geval betrekking hebben op:

- a. transport van Persoonsgegevens;
- b. fysieke en logische (toegangs)beveiliging tot apparatuur en systemen;
- c. logging, monitoring en controle op het netwerk en systemen;
- d. beheer(sing) van technische kwetsbaarheden en (security) patches;
- e. de informatiebeveiligingsbewustwording van medewerkers;
- f. afhandelen van beveiligingsincidenten en datalekken;
- g. continuïteitsbeheer en back-up/restore maatregelen;
- h. vernietigen van gegevens bij vervangen of afvoeren van gegevensdragers;
- i. een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen.

Verwerker 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.

[Beveiligingsplan]

[Statement of compliance (inclusief statement of applicability)]

[Auditverklaring]

Bijlage 3 – Meldplicht Datalekken

ALGEMEEN

Deze bijlage 3 bij de Verwerkersovereenkomst bevat afspraken en de procedure voor het opvolgen van een Datalek.

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 Verwerker 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.

PROCEDURE

Verwerker is gehouden ieder Datalek onverwijld, maar uiterlijk binnen 24 uur na ontdekking, aan SVB te melden.

Verwerker is gehouden SVB op de hoogte te brengen van een mogelijk Datalek door middel van een melding aan Servicedesk.svb@svb.nl.

Verwerker zal in haar melding aan 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 Verwerker bespreken.