Bijlage J - Bepalingen Verwerkersovereenkomst Inschrijver

Inschrijver dient een Verwerkersovereenkomst aan te leveren die integraal voldoet aan de eisen van de Algemene verordening gegevensbescherming. In de Verwerkersovereenkomst dienen daarnaast minimaal de volgende bepalingen te worden opgenomen:

1. Opdrachtnemer verplicht zich passende maatregelen te nemen en te onderhouden tot technische en organisatorische beveiliging tegen onbevoegde toegang tot persoonsgegevens, verlies – d.w.z. Opdrachtnemer waarborgt beschikbaarheid, integriteit en vertrouwelijkheid van de dienstverlening en daarop opgeslagen en/of verwerkte informatie – of tegen enige vorm van onrechtmatige verwerking van de persoonsgegevens, overeenkomstig art. 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 mediadragers;
   - een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen.
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 en NEN-ISO/ IEC 27002.
3. De in artikel 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.
4. Opdrachtnemer heeft de in artikel 1 bedoelde beveiligingsmaatregelen uitgewerkt in een informatiebeveiligingsplan dat als Bijlage J.a bij deze Verwerkersovereenkomst is bijgesloten. Gedurende de looptijd van de Raamovereenkomst beschikt Opdrachtnemer over een gecertificeerd informatiebeveiligingssysteem op basis van ISO/IEC 27001 dat is afgegeven door een onafhankelijke geaccrediteerde certificeringsinstantie, en dat betrekking heeft op de geleverde dienstverlening.
5. Minimaal jaarlijks levert Opdrachtnemer een recente formele audit-verklaring die past bij de aard van de gevraagde dienstverlening (zoals een ISAE 3402 type II rapportage of een ISAE 3000 rapportage op basis van één of meerdere SOC2 – Trusted Services Principes) 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 en het informatiebeveiligingsplan wordt aangetoond.
6. Opdrachtnemer 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. Opdrachtnemer zal hiertoe actuele ontwikkelingen volgen en additionele voorzieningen treffen voor zover dat redelijkerwijs van hem kan worden verwacht.

7. Opdrachtnemer voorziet SVB van de noodzakelijke informatie waardoor SVB een oordeel kan vormen over de naleving door Opdrachtnemer van de beveiligingsmaatregelen. Naast de genoemde rapportageverplichtingen in artikel 4, zal Opdrachtnemer eens per kwartaal samen met SVB het informatiebeveiligingsplan van Opdrachtnemer bespreken. In dit overleg zal Opdrachtnemer o.a. aanpassingen in het plan toelichten. Voor dit overleg brengt Opdrachtnemer geen kosten in rekening.
8. Opdrachtnemer meldt ieder datalek waarbij persoonsgegevens van SVB zijn betrokken onverwijld, maar uiterlijk binnen 24 uur na ontdekking, aan SVB. In Bijlage 1 is vastgelegd wanneer sprake is van een datalek en zijn afspraken gemaakt over de inhoud en verzending van de rapportage van datalekken. Indien Opdrachtnemer vaststelt dat sprake is van een datalek, zal zij alle noodzakelijke maatregelen treffen om verdere ontsluiting dan wel verspreiding van persoonsgegevens te voorkomen. Opdrachtnemer zal hiertoe in overleg treden met SVB en de aanwijzingen van SVB direct opvolgen. Opdrachtnemer zal SVB steeds op de hoogte houden van de ontwikkelingen met betrekking tot het datalek en de maatregelen die zij treft en heeft getroffen om de gevolgen van het datalek te beperken en herhaling van het datalek te voorkomen. Opdrachtnemer werkt op aangeven van 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.
9. 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. SVB kan de Audit 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. Indien de Audit aantoont dat Opdrachtnemer op een of meer punten tekortschiet in de naleving van deze Verwerkersovereenkomst, zijn de kosten van de Audit voor Opdrachtnemer. SVB zal de Audit tijdig aankondigen en de scope van de Audit vooraf met Opdrachtnemer bespreken. 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 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.
10. Opdrachtnemer is zich er bewust van dat de SVB in het kader van haar dienstverlening zeer vertrouwelijke persoonsgegevens verwerkt en dat de SVB als uitvoerende organisatie niet alleen een wettelijk maar ook een groot maatschappelijk belang heeft bij correcte naleving door Opdrachtnemer van deze Verwerkersovereenkomst. SVB verlangt daarom waarborgen van Opdrachtnemer en om die reden legt SVB aan Opdrachtnemer bij overtreding van de verplichtingen vastgelegd in deze Verwerkersovereenkomst ten gunste van SVB een direct opeisbare boete op van € 10.000 (tien duizend euro) per overtreding en van € 2.500 (twee en een half duizend euro) voor iedere dag (of deel daarvan) dat deze overtreding voortduurt. Zulks laat onverlet het recht van SVB om volledige schadevergoeding van Opdrachtnemer te vorderen.

Bijlage 1 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). Bij een datalek zijn persoonsgegevens blootgesteld aan verlies of onrechtmatige verwerking – dus aan datgene, waartegen de beveiligingsmaatregelen bescherming moesten bieden.

De Autoriteit Persoonsgegevens (AP) stelt dat een inbreuk in verband met persoonsgegevens ruim moet worden geduid. Het betreft alle beveiligingsincidenten waardoor de bescherming van persoonsgegevens op enig moment is doorbroken waardoor de persoonsgegevens zijn blootgesteld aan verlies of onrechtmatige verwerking. 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 had getroffen. Wel zijn deze maatregelen van belang voor de verplichting het datalek te melden bij de AP en/of betrokkenen. Indien de bij het datalek betrokken persoonsgegevens onbegrijpelijk of ontoegankelijk zijn gemaakt voor eenieder die geen recht heeft op kennisname van de gegevens, hoeft het datalek niet te worden gemeld bij de AP en/of betrokkenen. Het datalek levert dan geen risico op voor de rechten en vrijheden van natuurlijke personen. Het datalek wordt in een dergelijk geval wel aan de SVB gemeld, welke de meldingsplicht per datalek zal 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 SVB te melden. Het is enkel en alleen aan SVB om te bepalen of al dan geen sprake is van een (meldplichtwaardig) datalek.

Opdrachtnemer is gehouden SVB op de hoogte te brengen van een datalek door middel van een melding aan: Servicedesk SVB (servicedesk@svb.nl, 020-656 5777)

Opdrachtnemer 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 Opdrachtnemer bespreken.