

Bijlage 1a

Verplichtingen met betrekking tot Informatiebeveiliging aanvullend

Restauratiefonds en Leverancier komen het volgende overeen, dit in aanvulling op hetgeen verder is overeengekomen tussen partijen.

1 Algemeen

1. De Leverancier stemt ermee in dat het Restauratiefonds een 'right to audit' heeft met inbegrip van informatiebeveiligingsmaatregelen.
2. De Leverancier houdt zich aan de relevante wet –en regelgeving waaronder de AVG en verplicht zich taken te verrichten binnen het verwerkingsdoel.
3. De Leverancier stelt zich op de hoogte van en houdt zich aan de getekende verwerkingsovereenkomsten, vertrouwelijkheids- en geheimhoudingsovereenkomsten van het Restauratiefonds.
4. De Leverancier stemt in met de CDD toetsing door het Restauratiefonds.
5. De Leverancier kan desgevraagd aantonen dat bij het Restauratiefonds geplaatste medewerkers voldoende getraind zijn in informatiebeveiligingsmaatregelen en geven wisselingen in medewerkers tijdig door.

2 Persoonsgegevens en andere data

1. De Leverancier houdt zich aan de principes van data minimalisatie zodat alleen de benodigde data gezien en verwerkt wordt, waar hiertoe bevoegd voor een zo kort mogelijke termijn.
2. De Leverancier neemt passende technische en organisatorische maatregelen om gegevens van het Restauratiefonds te beveiligen. Deze maatregelen zijn afgestemd op het risico van de verwerking. Hieronder vallen ten minste:
 - a. De Leverancier maakt een back-up van de gegevens om te verzekeren dat het eventuele verlies van gegevens niet meer dan één dag bedraagt. De back-ups worden op een veilige locatie bewaard;
 - b. De Leverancier treft aantoonbaar de nodige voorzieningen, waaronder een bedrijfscontinuïteitsplan, zodat de gevolgen van een verstoring in de verwerking tot een minimum beperkt zullen blijven;
 - c. De Leverancier meldt een storing in de verwerking die langer dan vier uur duurt onmiddellijk aan het Restauratiefonds (ICT afdeling);
 - d. De Leverancier treft voorzieningen voor een adequate toegangsbeveiliging tot de voor de werkzaamheden relevante gegevens, zodat alleen geautoriseerd personeel toegang kan verkrijgen en houdt een lijst bij van geautoriseerd personeel;
 - e. De Leverancier heeft een adequaat en up to date mechanisme in werking om kwaadaardige software, waaronder computervirussen, te detecteren en adequaat af te handelen;
 - f. De Leverancier zal het Restauratiefonds direct op de hoogte stellen van relevante wijzigingen in de verwerkingsprocessen;
 - g. De Leverancier heeft in het algemeen op het gebied van informatiebeveiliging aantoonbare controlemechanismen in gebruik en kan deze op verzoek overleggen met inbegrip van relevante certificaten zoals de ISO 27001/27002 norm of een door het Restauratiefonds geaccepteerd equivalent.
3. Het Restauratiefonds is gerechtigd een rapportage op te vragen waarin de genomen beveiligingsmaatregelen vermeld staan en eventuele aandachtspunten zijn opgenomen.

4. De door de Leverancier te verwerken gegevens, op welke wijze dan ook verkregen, blijven eigendom van het Restauratiefonds.
5. De Leverancier geeft incidenten of ander informatiebeveiligingsbreuken direct door aan de Compliance Officer en Servicemanager van het Restauratiefonds en zo mogelijk niet later dan 24 uur nadat derde ervan kennis heeft gekregen. De Leverancier dient alle noodzakelijk informatie en medewerking te verlenen om het Restauratiefonds in staat te stellen zo spoedig mogelijk de oorzaak en de omvang hiervan vast te stellen. De Leverancier volgt hierbij de instructies van het Restauratiefonds op en maakt gebruik van de door het Restauratiefonds vastgestelde formulieren, zodat het Restauratiefonds op adequate wijze melding kan doen.
6. De Leverancier is verantwoordelijk om de vereisten en verplichtingen op het gebied van informatiebeveiliging door de gehele leveringsketen van dienstverlening door te voeren en op te leggen. Onaangename partijen die een rol hebben in de leveringsketen. Derde partij draagt zorg voor een sluitend overzicht van alle partijen in de keten. Deze ketenverantwoordelijkheid dient aantoonbaar te zijn inclusief afhankelijkheden en (sub)verwerkers. Het bewijs hiervoor wordt periodiek overlegd aan het Restauratiefonds.
 - a. De Leverancier mag zonder voorafgaande schriftelijke toestemming van het Restauratiefonds geen andere partijen (sub-verwerkers) inschakelen bij het verwerken van de Persoonsgegevens.
 - b. Indien de Leverancier met toestemming van het Restauratiefonds een andere partij inschakelt bij de verwerking van persoonsgegevens, dan moet deze partij voldoen aan de eisen die in de Verwerkersovereenkomst zijn opgenomen. Het Restauratiefonds kan aanvullende voorwaarden stellen aan de verwerking door andere partijen/sub-verwerkers. Voormelde eisen uit de Verwerkersovereenkomst, eventueel aangevuld met voorwaarden zoals in de vorige zin bedoeld, worden in een sub-verwerkersovereenkomst tussen derde en sub-verwerker vastgelegd. De Leverancier is jegens het Restauratiefonds aansprakelijk voor een correcte nakoming door de sub-verwerker van de verplichtingen uit bedoelde sub-verwerkersovereenkomst.
7. De Leverancier verwerkt alleen de persoonsgegevens na schriftelijke opdracht en instructie van het Restauratiefonds, heeft geen zeggenschap over het doel en de middelen voor de verwerking van persoonsgegevens en neemt geen beslissingen over het gebruik van de persoonsgegevens, de verstrekking aan andere partijen en de duur van de opslag van persoonsgegevens.
8. De Leverancier verschaft enkel toegang tot de persoonsgegevens aan haar werknemers voor zover dit nodig is voor het verrichten van de diensten. Onbevoegden hebben hier geen toegang toe.
9. De Leverancier voldoet desgevraagd aan een gerechtvaardigd verzoek van een betrokkene die zijn of haar wettelijke privacy-rechten wil uitoefenen. Deze rechten bestaan uit een verzoek om inzage, verbetering, aanvulling, verwijdering, afscherming, bezwaar maken tegen de verwerking van de persoonsgegevens en een verzoek tot overdraagbaarheid van de eigen persoonsgegevens.
10. De Leverancier verwerkt zonder expliciete en voorafgaande schriftelijke toestemming van Het Restauratiefonds geen persoonsgegevens, geheel of gedeeltelijk, buiten de Europese Economische Ruimte (EER).
11. De Leverancier is verplicht om na afloop van de overeenkomst de persoonsgegevens uit de systemen te verwijderen (met inbegrip van back-ups en logbestanden) conform het retentiebeleid van het Restauratiefonds. Tijdig voor het moment van beëindiging van de

overeenkomst, zullen zal in overleg gekeken worden of en op welke wijze de verwerkte gegevens aan het Restauratiefonds terug worden gegeven.