Verwerkersovereenkomst

STKKR verwerkt in sommige gevallen persoonsgegevens voor en in opdracht van de klant omdat de klant een software gebruikersovereenkomst (abonnement) met STKKR heeft. STKKR en de klant zijn daarom verplicht volgens de Algemene Verordening Gegevensbescherming (AVG) om een Verwerkersovereenkomst te sluiten. Omdat STKKR een standaard applicatie levert, heeft STKKR de verwerkingsovereenkomst opgenomen naast de Algemene Voorwaarden. STKKR is in deze de 'verwerker' en de klant de 'verwerkingsverantwoordelijke'. STKKR en de klant verplichten zich over en weer om de Algemene Verordening Gegevensbescherming (AVG) na te leven. Voor de definities van begrippen wordt aangesloten bij de AVG. STKKR zal de persoonsgegevens alleen verwerken voor en in opdracht van de klant en om uitvoering te geven aan de overeenkomst / het abonnement.

Toepasselijkheid en looptijd
Deze overeenkomst is van toepassing op iedere Verwerking die door Verwerker wordt gedaan op basis van de onderliggende overeenkomst tussen partijen. Deze overeenkomst treedt in werking op de datum waarop de onderliggende opdracht van kracht wordt en eindigt op hetzelfde moment als de onderliggende opdracht. Het is niet mogelijk om deze overeenkomst los van de onderliggende opdracht tussentijds op te zeggen.

De geheimhoudingsplicht zoals vastgelegd in deze overeenkomst blijft gelden, ook nadat het abonnement is beëindigd.

Instructies verwerking
De verwerking bestaat uit het beschikbaar stellen van de STKKR applicatie met als doel data van de klant in AFAS te kunnen toevoegen, aanpassen of verwijderen. De instructie hiertoe wordt via de applicatie gegeven.

Binnen de applicatie die STKKR beschikbaar stelt, kunnen er door de verwerkersverantwoordelijke regels worden ingegeven voor het bewerken van verschillende soorten gegevens (dus ook persoonsgegevens). De klant is zelf verantwoordelijk voor de beoordeling of het doel en aard van de verwerking past bij de diensten die STKKR verleent en dient zich hierbij aan geldende wet en regelgeving te houden.

STKKR verzamelt geanonimiseerde gegevens over het gebruik van haar producten en diensten. Deze gegevens ondersteunen STKKR om inzicht te krijgen of, hoe en hoe vaak bepaalde onderdelen van het product gebruikt worden. De geanonimiseerde gegevens zullen uitsluitend gebruikt worden om producten en dienstverlening te verbeteren. STKKR zal de verzamelde gebruikersstatistieken nooit gebruiken voor commerciële doeleinden of aanbieden aan derde partijen.

Geheimhoudingsplicht
STKKR is zich ervan bewust dat de informatie die de klant met STKKR deelt en opslaat binnen STKKR, een geheim en bedrijfsgevoelig karakter heeft. Alle (door STKKR ingeschakelde) medewerkers zullen gedurende hun dienstverband en daarna, zoals in hun arbeidsovereenkomst met

geheimhoudingsclausule is opgenomen, op verantwoorde wijze met de informatie van de klant omgaan.

Medewerkers met toegang tot klantgegevens
Systeembeheerders van STKKR hebben volledige toegang tot de gegevens die door de klant zijn ingevoerd, ten dienste van:

- het plaatsen van een nieuwe versie;
- het doorvoeren van patches en hotfixes;
- het maken van een back-up;

Beveiliging
STKKR neemt blijvend passende technische en organisatorische maatregelen om de gegevens van de klant en de software te beveiligen tegen verlies of enige vorm van onrechtmatige verwerking. Tevens is er een responsible disclosure opgenomen (https://stkkr.nl/responsible-disclosure/) om eventuele zwakke plekken zo goed mogelijk te kunnen opsporen en verhelpen.

Deze maatregelen worden aangemerkt als een passend beveiligingsniveau in de zin van de AVG.

Subverwerkers
De STKKR software draait in datacenters van https://www.oxilion.nl/oplossing/private-cloud-hosting/ en deze is in het geval dat er persoonsgegevens worden verwerkt subverwerker. De datacenters waar STKKR gebruik van maakt bevinden zich uitsluitend in Nederland en vallen onder Nederlandse wet- en regelgeving en voldoen aan de strenge Nederlandse en Europese wetgeving met betrekking tot logische en fysieke toegangsbeveiliging en continuïteit. De datacenters zijn minimaal ISO 27001 gecertificeerd. De (persoons)gegevens worden door STKKR en subverwerker uitsluitend verwerkt binnen de Europese Economische ruimte.

STKKR zal geen nieuwe subverwerkers gegevens laten verwerken zonder 1)de klant daarover tijdig te informeren en 2) hen contractueel dezelfde wettelijke verplichtingen op te leggen zoals die ook in deze verwerkersovereenkomst zijn vervat, met name maar niet beperkt tot de bepalingen uit artikel 28 AVG. De klant kan bezwaar maken bij STKKR tegen de subverwerker. STKKR zal deze bezwaren op directieniveau afhandelen. Mocht STKKR toch gegevens willen laten verwerken door de nieuwe subverwerker, heeft de klant de mogelijkheid om de overeenkomst te beëindigen.

Privacyrechten
STKKR heeft geen zeggenschap over de persoonsgegevens die door de klant beschikbaar worden gesteld. Zonder noodzaak, gezien de aard van de door de klant verstrekte opdracht, expliciete toestemming van de klant of wettelijke verplichting zal STKKR de gegevens niet aan derden verstrekken of voor andere doeleinden verwerken, dan voor de overeengekomen doeleinden. De klant garandeert dat de persoonsgegevens verwerkt mogen worden op basis van een in de AVG genoemde grondslag.

Betrokkenen
De klant is verantwoordelijk voor de ingevoerde gegevens van de betrokkenen en daarbij voor het

informeren en bijstaan van de rechten van de betrokkenen. STKKR zal nooit op verzoeken van betrokkenen ingaan en altijd verwijzen naar de verantwoordelijke. STKKR zal, voor zover dat binnen de applicatie mogelijk is, haar medewerking verlenen aan de klant zodat deze kan voldoen aan zijn wettelijke verplichtingen in het geval dat een betrokkene haar rechten uitoefent op grond van de AVG of andere toepasselijke regelgeving betreffende de verwerking van persoonsgegevens (zoals het recht op inzage, correctie, vergetelheid en dataportabiliteit).

Uitvoeren DPIA

STKKR (verwerker) zal de klant (verwerkersverantwoordelijke) voor zover mogelijk bijstand verlenen bij het vervullen van de plicht van de laatste om in gevallen waarbij de verwerking waarschijnlijk een hoog risico voor de privacy van Betrokkenen inhoudt;

- een Privacy Impact Assessment (DPIA) uit te voeren;
- de Autoriteit voorafgaand raad te plegen.

Verwerker kan hiervoor kosten bij Verwerkingsverantwoordelijke in rekening brengen.

Meldplicht datalekken

De AVG vereist dat eventuele datalekken gemeld worden aan de Autoriteit Persoonsgegevens door de verwerkingsverantwoordelijke van de data. STKKR zal daarom zelf geen meldingen doen bij de Autoriteit Persoonsgegevens. Uiteraard zal STKKR de klant juist, tijdig en volledig informeren over relevante incidenten, zodat de klant als verwerkingsverantwoordelijke aan zijn wettelijke verplichtingen kan voldoen. De Beleidsregels meldplicht datalekken van de Autoriteit Persoonsgegevens geven hierover meer informatie.

Bepaling datalek
Voor het bepalen van een datalek, gebruikt STKKR de AVG en de Beleidsregels meldplicht datalekken als leidraad.

Melding aan de klant
Indien blijkt dat bij STKKR sprake is van een beveiligingsincident of datalek zal STKKR de klant daarover zo spoedig mogelijk informeren nadat STKKR bekend is geworden met het datalek. Om dit te realiseren zorgt STKKR ervoor dat al haar medewerkers in staat zijn en blijven om een datalek te constateren en verwacht STKKR van haar opdrachtnemers dat zij STKKR in staat stelt om hier aan te kunnen voldoen. Voor de duidelijkheid: als er een datalek is bij een leverancier van STKKR, dan meldt STKKR dit uiteraard ook. STKKR is het contactpunt voor de klant. De klant hoeft geen contact op te nemen met de leveranciers van STKKR.

Informeren klant (contactpersoon instellen)
In eerste instantie zal STKKR de *contactpersoon van het contract* informeren over een datalek. Mocht deze contactpersoon niet (meer) de juiste zijn, dan kan dat aangepast worden via de klantportal bij de organisatiegegevens.

Informatie verstrekken
STKKR probeert de klant direct alle informatie te verstrekken die de klant nodig heeft om een eventuele melding bij de Autoriteit Persoonsgegevens en/of de betrokkene(n) te verrichten.

Termijn van informeren
De AVG geeft aan dat er 'onverwijld' gemeld moet worden. Dit is volgens de Autoriteit Persoonsgegevens zonder onnodige vertraging en zo mogelijk niet later dan 72 uur na ontdekking ervan door de verantwoordelijke. Indien er een beveiligingsincident optreedt zal STKKR de klant zo snel mogelijk, maar uiterlijk binnen 48 uur na het ontdekken door STKKR ervan, informeren. De klant zal zelf de beoordeling moeten maken of het beveiligingsincident valt onder de term 'datalek' en of er melding aan de Autoriteit Persoonsgegevens gedaan zal moeten worden. Vanaf het moment dat de klant op de hoogte is gesteld van een beveiligingsincident heeft hij 72 uur de tijd om dit te melden aan de Autoriteit.

Voortgang en maatregelen
STKKR zal de klant op de hoogte houden over de voortgang en de maatregelen die getroffen worden. STKKR maakt hierover afspraken met de primaire contactpersoon bij de initiële melding. In ieder geval houdt STKKR de klant op de hoogte in geval van een wijziging van de situatie, het bekend worden van nadere informatie en over de maatregelen die getroffen worden.

Gegevens verwijderen
STKKR zal, na afloop van het abonnement, alle klantgegevens verwijderen. Alle stkkrs, en AFAS omgeving gerelateerde data van de klant worden per direct, volledig verwijderd.

Controlerecht
De klant heeft het recht om periodiek, doch maximaal één (1) keer per jaar, een audit uit te laten voeren door een gekwalificeerd auditor om na te gaan of Verwerker haar verplichtingen uit hoofde van deze Verwerkersovereenkomst nakomt (hierna: "Audit"). De auditor is aan geheimhouding gebonden. Verwerker zal, waar mogelijk, verbeterpunten van de auditor uitvoeren. Dit maximum van één keer per jaar geldt niet wanneer er naar mening van de klant onderbouwde aanwijzingen zijn dat Verwerker tekort schiet in haar technische en/of organisatorische informatiebeveiliging.

Verwerker en de door haar ingeschakelde sub-Verwerkers/onderaannemers die Persoonsgegevens verwerken, zullen aan de klant toegang verlenen en alle informatie verschaffen die redelijkerwijs geëist kan worden en die relevant is voor de verwerking van de Persoonsgegevens. Verwerker zal in dat kader alle medewerking verlenen die redelijkerwijs nodig is.

De kosten van een Audit komen voor rekening van de klant, tenzij blijkt dat Verwerker of een door haar ingeschakelde sub-Verwerker/onderaannemer haar beveiligingsverplichtingen niet of niet-volledig is nagekomen.

Indien uit het auditrapport blijkt dat de door Verwerker getroffen maatregelen en voorzieningen niet in voldoende mate voldoen aan de geldende wet- en/of regelgeving zal Verwerker onverwijld de nodige maatregelen treffen om hier alsnog aan te voldoen.

Verwerker is verplicht mee te werken aan verzoeken om informatie of het houden van onderzoek door of namens toezichthouders zoals de Autoriteit Persoonsgegevens, de Autoriteit Consument & Markt, De Nederlandsche Bank en de Autoriteit Financiële Markten. Verwerker volgt aanwijzingen van de toezichthouder op. Verwerker verstrekt de klant, indien de wet dit toestaat, een kopie van de gegevens die zij de toezichthouder heeft gegeven.