

# Silvasoft Verwerkersovereenkomst (AVG)

Versie: 1.1

Laatst gewijzigd op: 20-06-2023

## Betrokken partijen:

1. Het individu of de rechtspersoon die een abonnement op de Silvasoft software heeft en daarvoor een overeenkomst met Silvasoft heeft hierna te noemen: Opdrachtgever,

en

2. Silvasoft, (statutair) gevestigd te Ridderkerk, hierna te noemen: Wederpartij,

hierna gezamenlijk te noemen: Partijen;

## OVERWEGENDE DAT:

- Voor zover Wederpartij Persoonsgegevens verwerkt ten behoeve van Opdrachtgever in het kader van de Overeenkomst kwalificeert Opdrachtgever krachtens artikel 4, onderdeel 7 en onderdeel 8, van de Verordening als verwerkingsverantwoordelijke voor de Verwerking van Persoonsgegevens en Wederpartij als verwerker;
- Partijen in deze Verwerkersovereenkomst, zoals bedoeld in artikel 28, derde lid, van de Verordening, hun afspraken over de Verwerking van Persoonsgegevens door Wederpartij wensen vast te leggen.

## KOMEN OVEREEN:

### Artikel 1. Begrippen

In deze Verwerkersovereenkomst wordt een aantal begrippen met een beginhoofdletter gebruikt. Aan deze begrippen komt de volgende betekenis toe:

- 1.1 Betrokkene: degene op wie een Persoonsgegeven betrekking heeft.
- 1.2 Inbreuk in verband met Persoonsgegevens: 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.
- 1.3 Overeenkomst: de overeenkomst tussen Opdrachtgever en Wederpartij, zijnde de meest recente zoals deze gedeeld wordt per e-mail en tevens is terug te vinden in de Silvasoft applicatie via het menu Beheer.
- 1.4 Persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon, die Wederpartij in het kader van de Overeenkomst ten behoeve van Opdrachtgever verwerkt.
- 1.5 Verordening: Verordening (EU) 2016/679 van het Europees Parlement en de Raad 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 de Richtlijn 95/46/EG (algemene verordening gegevensbescherming).
- 1.6 Verwerkersovereenkomst: deze overeenkomst inclusief overwegingen en bijbehorende bijlagen.

1.7 Verwerking: een bewerking of een geheel van bewerkingen in het kader van de Overeenkomst met betrekking tot Persoonsgegevens, of een geheel van Persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen.

#### Artikel 2. Voorwerp van deze Verwerkersovereenkomst

2.1 Deze Verwerkersovereenkomst regelt de Verwerking van Persoonsgegevens door Wederpartij in het kader van de Overeenkomst.

2.2 De aard en het doel van de Verwerking, het soort Persoonsgegevens en de categorieën van Betrokkenen zijn in Bijlage 1 omschreven.

2.3 Wederpartij garandeert de toepassing van passende technische en organisatorische maatregelen, opdat de Verwerking aan de vereisten van de Verordening voldoet en de bescherming van de rechten van de Betrokkene is gewaarborgd.

2.4 Wederpartij garandeert te voldoen aan de vereisten van de toepasselijke wet- en regelgeving betreffende de verwerking van Persoonsgegevens.

#### Artikel 3. Inwerkingtreding en duur

3.1 Deze Verwerkersovereenkomst treedt in werking op het moment dat hiertoe via de Silvasoft applicatie akkoord is gegeven door Opdrachtgever.

3.2 Deze Verwerkersovereenkomst eindigt nadat en voor zover Wederpartij alle Persoonsgegevens overeenkomstig artikel 10 heeft gewist of terugbezorgd.

3.3 Geen van Partijen kan deze Verwerkersovereenkomst tussentijds opzeggen.

#### Artikel 4. Omvang Verwerkingsbevoegdheid Wederpartij

4.1 Wederpartij Verwerkt de Persoonsgegevens uitsluitend in opdracht van Opdrachtgever behoudens afwijkende wettelijke voorschriften die op Wederpartij van toepassing zijn.

4.2 Indien een instructie als bedoeld in het eerste lid naar het oordeel van Wederpartij in strijd is met een wettelijk voorschrift inzake gegevensbescherming, stelt hij Opdrachtgever daarvan voorafgaand aan de verwerking in kennis, tenzij een wettelijk voorschrift deze kennisgeving verbiedt.

4.3 Indien Wederpartij op grond van een wettelijke verplichting Persoonsgegevens dient te verstrekken, informeert hij Opdrachtgever onmiddellijk, en zo mogelijk voorafgaand aan de verstrekking.

4.4 Wederpartij heeft geen zeggenschap over het doel van en de middelen voor de Verwerking van Persoonsgegevens.

#### Artikel 5. Beveiliging van de Verwerking

5.1 In aanvulling op de beschreven maatregelen in de Algemene Voorwaarden en het Service Level Agreement van Wederpartij treft Wederpartij de technische en organisatorische beveiligingsmaatregelen zoals beschreven in Bijlage 2.

5.2 Partijen erkennen dat het waarborgen van een passend beveiligingsniveau voortdurend kan dwingen tot het treffen van aanvullende beveiligingsmaatregelen. Wederpartij waarborgt een op het risico afgestemd beveiligingsniveau.

5.3 Indien en voor zover Opdrachtgever daarom uitdrukkelijk schriftelijk verzoekt, zal wederpartij aanvullende maatregelen treffen met het oog op de beveiliging van de Persoonsgegevens indien dit verzoek gegrond wordt bevonden door Wederpartij.

5.4 Wederpartij Verwerkt Persoonsgegevens niet buiten de Europese Unie, tenzij hij daarvoor uitdrukkelijk schriftelijk toestemming heeft verkregen van Opdrachtgever en behoudens afwijkende wettelijke verplichtingen.

5.5 Wederpartij informeert Opdrachtgever zonder onredelijke vertraging zodra hij kennis heeft genomen van onrechtmatige Verwerkingen van Persoonsgegevens of inbreuken op beveiligingsmaatregelen zoals genoemd in het eerste en tweede lid.

5.6 Wederpartij verleent Opdrachtgever bijstand bij het doen nakomen van de verplichtingen uit hoofde van de artikelen 32 tot en met 36 van de Verordening.

#### Artikel 6. Geheimhouding door Personeel van Wederpartij

6.1 De Persoonsgegevens hebben een vertrouwelijk karakter.

6.2 Wederpartij toont op verzoek van Opdrachtgever aan dat zijn Personeel zich ertoe heeft verbonden vertrouwelijkheid in acht te nemen.

#### Artikel 7. Subverwerker

Wanneer Wederpartij een andere verwerker inschakelt om ten behoeve van Opdrachtgever verwerkingsactiviteiten te verrichten, worden aan deze andere verwerker bij een overeenkomst dezelfde verplichtingen inzake gegevensbescherming opgelegd als die welke in deze Verwerkersovereenkomst zijn opgenomen.

Het staat Wederpartij vrij om subverwerkers in te schakelen zolang aan deze overeenkomst wordt voldaan door de subverwerkers.

Lijst van subverwerkers \*:

**Google Cloud Platform:** hosting, backups

**Amazon S3 + Amazon Glacier:** file storage, backups

**Klipppa:** Scan & Herken + Mail & Herken

**Upvoty:** Feedback portal

**SendGrid:** E-mail service

**Zendesk:** Support systeem (e-mail communicatie met Opdrachtgever)

**Ponto:** Bankenkoppeling

**ING Bank:** Automatische incasso licentiekosten Opdrachtgever

**PayQ:** Incassobureau betalingsopvolgingen

**Moosend:** E-mails / nieuwsbrieven

\*Sommige subverwerkers zijn enkel relevant indien u gebruik maakt van de relevante functionaliteit in Silvasoft.

In bijlage II wordt meer informatie gegeven over technische en organisatorische maatregelen rondom waarborging van gegevens.

#### Artikel 8. Bijstand vanwege rechten van Betrokkene

Wederpartij verleent Opdrachtgever bijstand bij het vervullen van diens plicht om verzoeken om uitoefening van de in hoofdstuk III van de Verordening vastgestelde rechten van de Betrokkene te beantwoorden.

## Artikel 9. Inbreuk in verband met Persoonsgegevens

9.1 Wederpartij informeert Opdrachtgever zonder onredelijke vertraging, zodra hij kennis heeft genomen van een Inbreuk in verband met Persoonsgegevens, overeenkomstig de afspraken zoals vastgelegd in Bijlage 3.

9.2 Wederpartij informeert Opdrachtgever ook na een melding op grond van het eerste lid over ontwikkelingen betreffende de Inbreuk in verband met Persoonsgegevens.

9.3 Partijen dragen de door henzelf in verband met de melding aan de bevoegde toezichthoudende autoriteit en Betrokkene te maken kosten.

9.4 Opdrachtgever is zelf verantwoordelijk voor het melden van datalekken omdat Opdrachtgever de verwerkingsverantwoordelijke is. Een melding wordt pas gemaakt nadat Silvasoft is geïnformeerd en nadat Silvasoft het incident heeft kunnen onderzoeken en een reactie aan Opdrachtgever is verstrekt. Deze reactie wordt binnen 2 werkdagen gegeven.

## Artikel 10. Teruggave Persoonsgegevens

10.1 Opdrachtgever is zelf verantwoordelijk om voor het beëindigen van de overeenkomst een export te maken van de gegevens indien Opdrachtgever deze wenst te bewaren. Wederpartij biedt daartoe diverse Export mogelijkheden.

10.2 Wederpartij zal gegevens van Opdrachtgever verwijderen na de geldende wettelijke bewaarplicht. Indien gewenst kan Opdrachtgever deze bewaarplicht overnemen door de exports te bewaren. Indien hiertoe een aanvullende overeenkomst opgesteld wordt tussen Opdrachtgever en Wederpartij zal Wederpartij de gegevens direct daarna verwijderen.

10.3. Na het verwijderen van de gegevens is het mogelijk dat gegevens toch nog aanwezig zijn in back-ups die door Wederpartij worden gemaakt. Deze back-ups worden niet langer bewaard dan beschreven in het Service Level Agreement.

## Artikel 11. Informatieverplichting en audit

11.1 Wederpartij stelt alle informatie ter beschikking die nodig is om aan te tonen dat de verplichtingen uit deze Verwerkersovereenkomst zijn en worden nagekomen.

11.2 Wederpartij verleent alle benodigde medewerking aan audits. Kosten voor dergelijke audits zijn voor rekening van Opdrachtnemer.

## **Ondertekening**

Ondertekening van dit document heeft plaatsgevonden via de Silvasoft applicatie waar Opdrachtgever akkoord heeft gegeven.

## **Bijlage 1. De Verwerking van Persoonsgegevens**

Het onderwerp/aard en doel van de Verwerking	Het doel van de verwerking is gezien de aard van de Silvasoft software velerlei en bij Wederpartij onbekend. Dit kan zijn t.b.v. CRM, financiële administratie, Sales, Marketing, etc.
Het soort Persoonsgegevens	N.a.w. gegevens, contact gegevens, notities, logging, facturatie, etc.

Beschrijving categorieën Persoonsgegevens	Voornamelijk gewone persoonsgegevens. Alhoewel het de Opdrachtgever mogelijk is om ook bijzondere persoonsgegevens vast te leggen.
Beschrijving categorieën Betrokkenen	Personen, organisaties
Beschrijving categorieën ontvangers van Persoonsgegevens	Vanuit het perspectief van Wederpartij slechts de verwerkingsverantwoordelijke. Dit zijn eveneens organisaties, personen en/of systemen (via de Silvasoft API).

## Bijlage 2. Passende technische en organisatorische maatregelen

Hier onder een niet limitatieve opsomming van maatregelen die door Silvasoft wordt genomen om uw gegevens te beschermen:

### Organisatorische maatregelen Silvasoft:

- Binnen Silvasoft werken we o.b.v. een need-to-know basis en hebben we een duidelijke functieonderscheiding. Op database niveau betekent dit dat er maar enkele personen zijn die daadwerkelijk bij de productiedatabase kunnen komen (beheerder/ontwikkelaar). De toegang tot de productiedatabase is beveiligd en afgeschermd. Onze support desk kan niet bij de database komen.
- Op applicatie niveau hebben we ook verregaande beveiliging van uw gegevens doorgevoerd. Silvasoft kent geen 'superusers'. Er is dus geen enkele medewerker van Silvasoft die via de applicatie in uw 'mijn-Silvasoft' kan inloggen. Enkel wanneer u ons expliciet toegang geeft kan een medewerker meekijken in uw administratie.
- Op testomgevingen werken we zoveel mogelijk met testdata. De testomgeving draait eveneens in de Google Cloud. Indien het nodig is voor reproductie van issues/bugs kunnen we bij uitzondering gebruik maken van de productiedatabase. Deze wordt dan tijdelijk op een testomgeving geplaatst en weer verwijderd zodra het issue is opgelost.
- De workstations van onze medewerkers zijn beveiligd en maken gebruik van o.a. Bitlocker voor de encryptie van schijven.
- We gebruiken binnen Silvasoft geen transferabele media (USB sticks, externe schrijven, etc.).
- We hebben geschreven procedures voor indiensttreding en uitdiensttreding van medewerkers zodat de toegang correct wordt ingeregeld en correct wordt ontnomen.

### Technische maatregelen Silvasoft:

- Toegang tot uw Silvasoft omgeving kan beschermt worden met 2FA. Dit is uw eigen keuze maar zal een extra laag van bescherming bieden.
- De Silvasoft website en applicatie draait o.b.v. SSL t.b.v. de beveiliging van al het verkeer tussen uw computer en de Silvasoft server.
- De Silvasoft applicatie maakt gebruik van het low-code platform Mendix. Dit platform heeft een ISMS geïmplementeerd conform de ISO/IEC 27001 standaard. Mendix heeft tientallen certificeringen m.b.t. beveiliging: <https://www.mendix.com/evaluation-guide/enterprise-capabilities/security/>
- Het Mendix platform wordt maandelijks onderworpen aan zogenaamde penetratietesters waarmee (goedwillende) hackers proberen in te breken op de Mendix Cloud. Als bewijs van

de technische en organisatorische maatregelen die Mendix ten aanzien van beveiliging hebben geïmplementeerd beschikt Mendix over diverse ISO, ISAE en NEN certificeringen.

- Silvasoft draait op recente versies van het Mendix low-code platform, Linux en PostgreSQL. Upgrades naar nieuwere versies gebeuren op regelmatige basis zodat de laatste beveiligingsmaatregelen geïmplementeerd zijn voor uw gegevens.

### Bijlage 3: Afspraken betreffende Inbreuken in verband met Persoonsgegevens

De Wederpartij zal bij een Inbreuk de Opdrachtgever informeren per e-mail. Het e-mailadres dat daarvoor gebruikt zal worden is degene die geregistreerd is in de Silvasoft applicatie als beheerder van de Opdrachtgever.

- Hierbij zal de volgende informatie worden verstrekt:
- Aard van de Inbreuk in verband met Persoonsgegevens
- De Persoonsgegevens en Betrokkene
- Waarschijnlijke gevolgen van de Inbreuk in verband met Persoonsgegevens
- Maatregelen die Wederpartij heeft voorgesteld of genomen om de Inbreuk in verband met Persoonsgegevens aan te pakken, waaronder, in voorkomend geval, de maatregelen ter beperking van de eventuele nadelige gevolgen daarvan

Opdrachtgever zal, indien deze zelf een inbreuk heeft geconstateerd Wederpartij direct informeren en instaat stellen de inbreuk te onderzoeken. Pas nadat dit onderzoek heeft plaats gevonden en de uitslag daarvan bekend (binnen 2 werkdagen) zal Opdrachtgever een evt. melding Datalek doen indien Opdrachtgever daartoe verplicht is.