

VSA bv

**Verwerkersovereenkomst
Support- en Beheer**



**Deel 1: Data Pro Statement
Deel 2: Standaardclausules voor verwerkingen**



VSA bv

Amerikaweg 8-4
9407 TK Assen

info@vsa.nl
www.vsa.nl

T: +31 (0)88 872 0 530

Documentbeschrijving

<i>Auteur</i>	Stephan de Boer
<i>Documentnaam</i>	vsa - verwerkersovereenkomst support en beheer.docx
<i>Eigenaar</i>	VSA bv
<i>Datum</i>	05-01-2023
<i>Classificatie</i>	Openbaar
<i>Status</i>	Definitief
<i>Versie</i>	2.0

Documenthistorie

<i>Versie</i>	<i>Toelichting</i>	<i>Auteur</i>	<i>Datum</i>
0.1	Concept	SdB	1-3-2018
1.0	Definitief	SdB	25-4-2018
1.1	ISO27001 en Data Pro toegevoegd	SdB	9-2019
1.2	Toevoeging: punt 10; ondersteuning bij verzoeken	JW	16-09-2021
1.3	Toevoeging ITG Software als sub-processor	JW	28-09-2021
1.4	Deel 1, punt 8; toevoeging niet EU-landen Toevoeging Telador als sub-processor	JW	15-02-2022
1.5	Toevoeging VSA IT-onderhoudscontract	JW	1-9-2022
2.0	Naams- en huisstijl wijzigingen	JW	5-1-2023

DEEL 1: DATA PRO STATEMENT

Dit Data Pro Statement vormt samen met de Standaardclausules voor verwerkingen (deel 2) de verwerkersovereenkomst voor de Support- en Beheerovereenkomst VSA bv.

ALGEMENE INFORMATIE

1. Dit Data Pro Statement is opgesteld door:

VSA bv

Amerikaweg 8-4

9407 TK Assen

Voor vragen over dit Data Pro Statement of dataprotectie kan contact opgenomen worden met: Johannes Werkman, +31 88 8720510, j.werkman@vsa.nl

2. Dit Data Pro Statement geldt vanaf 25 mei 2018

De in dit Data Pro Statement omschreven beveiligingsmaatregelen passen wij regelmatig aan om ten aanzien van data protectie steeds voorbereid en actueel te blijven. Wij houden u op de hoogte van nieuwe versies via onze normale kanalen.

3. Dit Data Pro Statement is van toepassing op de diensten van VSA die voortvloeien uit de: Support- en Beheerovereenkomst en VSA IT-onderhoudscontract

4. Omschrijving onderdelen uit Support- en Beheerovereenkomst

De supportovereenkomst van VSA bestaat uit de volgende onderdelen:

T Telefonische support (kantoor tijd)

4/8 4/8-uurs service op servers

R Remote beheer

S Systeembeheer

VOB VSA Online Backup

AV Antivirus

PCI Onderhoud PCI Compliance

VoIP Digitale telefonie

Deze modules worden uitgebreid beschreven in de Support- en Beheerovereenkomst.

Omschrijving onderdelen VSA IT-onderhoudscontract

IT Support en Beheer Telefonische support, Remote Beheer, Systeembeheer, Online Back-up, Antivirus

Advanced Security 24x7x365 opsporen van, reageren op en herstellen van cyber-security incidenten/dreigingen

Disaster Recovery Aanvullende bescherming en controles t.b.v. ransomware

Compliance Onderhoud PCI-DSS Compliance

Deze modules worden uitgebreid beschreven in het VSA IT-onderhoudscontract

5. Beoogd gebruik

Klanten sluiten een VSA IT-onderhoudscontract zodat VSA het gebruik van de automatiseringsomgeving (eigendom van de klant) kan ondersteunen en het systeembeheer hierop kan uitvoeren.

Bij deze dienst is geen rekening gehouden met de verwerking van bijzondere persoonsgegevens, of gegevens betreffende strafrechtelijke veroordelingen en strafbare feiten. Verwerken van deze gegevens met de hiervoor omschreven dienst door opdrachtgever is ter eigen beoordeling door opdrachtgever.

6. VSA heeft “privacy by design” op de volgende wijze toegepast:

Klanten bewerken zelf hun gegevens, inclusief door hen gekozen bijlagen en kunnen deze gegevens en documenten wijzigen en verwijderen. VSA controleert de gegevens niet en zal gegevens alleen inzien op verzoek van klant, bijvoorbeeld als dat nodig is om een vraag aan de servicedesk te beantwoorden.

7. VSA gebruikt de Data Pro Standaardclausules voor verwerkingen, welke in deel 2 te vinden zijn

8. VSA verwerkt de persoonsgegevens van zijn opdrachtgevers binnen de EU/EER en de landen die voldoen aan de adequaatheidseisen opgesteld door de Europese gegevensbeschermings-autoriteit.

9. VSA maakt gebruik van sub-processors:

Voor het uitvoeren van onze dienstverlening maken wij gebruik van subverwerkers. Een overzicht van deze subverwerkers is te vinden op <https://www.vsa.nl/subverwerkers>.

10. VSA ondersteunt de opdrachtgever op de volgende manier bij verzoeken van betrokkenen:

Het melden van storingen, correctie- en verwijderingsverzoeken kunnen worden aangevraagd worden per mail via onze servicedesk (support@vsa.nl) of via onze SelfServicePortal (<https://selfservice.vsa.nl>). Daarnaast zijn wij 24/7 telefonisch bereikbaar op telefoonnummer +31 88 8720530.

11. Na beëindiging van de overeenkomst met een opdrachtgever verwijdert VSA de persoonsgegevens die hij voor opdrachtgever verwerkt in principe binnen 3 maanden op zodanige wijze dat deze niet langer kunnen worden gebruikt en niet langer toegankelijk zijn (render inaccessible)

BEVEILIGINGSBELEID

12. VSA heeft de volgende beveiligingsmaatregelen genomen:

- Medewerkers van VSA hebben een geheimhoudingsverklaring ondertekend
- Medewerkers van VSA hebben een VOG-verklaring
- Medewerkers van VSA loggen in met individuele gebruikersnamen en wachtwoorden
- Medewerkers van VSA gebruiken tweeweg authenticatie om in te loggen
- Gebruik van disk encryptie bij laptops / notebooks
- Gebruik van softwarematige firewall (gebruikerssystemen)
- Implementatie van firewalls
- Wachtwoorden van VSA hebben minimale complexiteit
- Wachtwoorden van VSA worden periodiek gewijzigd
- Systemen van VSA maken gebruik van Endpoint Detection and Response
- Systemen van VSA maken gebruik van Intrusion-Detection-Software (IDS)
- Periodieke vulnerability scan
- Logfiles worden periodiek bekeken
- Gedocumenteerde procedure voor het intern melden van beveiligingsincidenten

13. VSA heeft zich geconformeerd aan het volgende Information Security Management System (ISMS):

- ISO 27001
- ISO 27701
- PCI/DSS

14. VSA heeft de volgende certificering:

- ISO 27001
- ISO 27701

DATALEKPROTOCOL

15. In geval er toch iets mis gaat, hanteert VSA het volgende datalekprotocol om ervoor te zorgen dat klanten op de hoogte zijn van incidenten:

Er is bij VSA een procedure voor het intern melden van incidenten. Indien VSA in zijn organisatie een datalek ontdekt, zal VSA zijn opdrachtgever daarvan zo snel mogelijk op de hoogte stellen, door contact op te nemen met de verantwoordelijke directeur en/of general manager. Eerst telefonisch, daarna door een email te sturen.

VSA levert zo veel mogelijk relevante gegevens aan, waaronder omschrijving van het incident, aard van de inbreuk, aard persoonsgegevens c.q. categorieën van betrokken data subjects, schatting van aantal betrokken data subjects en mogelijk betrokken databases, indicatie wanneer incident heeft plaatsgevonden.

Opdrachtgever kan met vragen terecht bij Johannes Werkman (zie gegevens bij punt 1). VSA zal aan Opdrachtgever een omschrijving geven van de genomen maatregelen om eventuele schade te beperken of om dit in de toekomst te voorkomen.

VSA zal aan Opdrachtgever een advies geven over de mogelijk te nemen maatregelen.

Meldingen worden indien mogelijk binnen 36 uur gedaan aan Opdrachtgever. VSA zal zelf geen meldingen doen aan AP of Data subjects. Wel of niet melden blijft de verantwoordelijkheid van de Opdrachtgever. VSA zal de opdrachtgever of de controller desgewenst ondersteunen bij het meldproces.