GEGEVENSVERWERKINGSOVEREENKOMST (GVO)

1. ALGEMEEN

1.1. Deze gegevensverwerkingsovereenkomst ("**GVO**") regelt de rechten en verplichtingen van Concrefy als verwerker en van de klant/opdrachtgever als verwerkingsverantwoordelijke in het kader van de verwerking van persoonsgegevens namens Concrefy.

1.2. Deze GVO is van toepassing op alle activiteiten waarbij de Verwerker of geautoriseerde onderaannemers (subverwerkers) persoonsgegevens van de Klant verwerken.

1.3. Termen die in deze GVO worden gebruikt, moeten worden begrepen in overeenstemming met hun definitie in de EU General Data Protection Regulation (GDPR).

1.4. De bepalingen van deze GVO zijn in overeenstemming met de **Algemene Verordening Gegevensbescherming (AVG)**, de Nederlandse implementatie van de GDPR. Waar in deze overeenkomst wordt verwezen naar de GDPR, wordt dit geacht tevens te verwijzen naar de overeenkomstige bepalingen van de AVG.

2. INHOUD VAN DE VERWERKING

2.1. De verwerking is gebaseerd op de tussen partijen (Offerte en Concrefy Algemene Voorwaarden) gesloten overeenkomst op grond waarvan de Verwerker aan de Klant bepaalde diensten levert bestaande uit softwareapplicaties, webportalen en bijbehorende ondersteunende onderdelen zoals advies, testen of onderhoud (de 'Overeenkomst'). In dit kader zal de Verwerker persoonsgegevens verwerken van Geautoriseerde Gebruikers/Gebruikers (doorgaans werknemers van de Klant), evenals van andere natuurlijke personen die betrokken zijn bij de operationele processen van de Klant, zoals werknemers van bouwbedrijven, onderaannemers, architecten, leveranciers, productiepartners of andere derden die door de Klant worden aangewezen of waarvan de gegevens door de Verwerker worden geüpload als verwerkingsverantwoordelijke, met het oog op het verlenen en leveren van de Concrefy-oplossingen en diensten/services.

2.2. De volgende gegevenscategorieën worden verwerkt ten behoeve van de verwerkingsverantwoordelijke: Naam, contactgegevens (zoals e-mailadres, telefoonnummers, etc), contractgegevens, inloggegevens (gebruikersnaam en wachtwoord), loggegevens (datum en tijd), geselecteerd besturingsapparaat, bedrijf, affiliatie en functie in het bedrijf, locatie, rol in de dienst, voorkeurstaal, logs (afbeeldingen) gegevens bij het aanvragen van ondersteunende diensten (bijv. "tickets").

2.3. Gegevens die zijn ingevoerd in de service voor testen, bouwprojecten en bouwlocaties van de Klant, meetgegevens, voorraadgegevens, gegevens over materiaalsamenstelling, artikelstamgegevens, financiële gegevens, bestelgegevens, vallen niet onder deze GVO

2.4. Het doel van de verwerking van persoonsgegevens is de uitvoering van de werkzaamheden die in de hoofdovereenkomst als diensten, services, prestaties of Concrefy oplossingen zijn gespecificeerd of waarvoor de Klant vervolgens instructies heeft gegeven aan de Verwerker.

2.5. De duur van de verwerking wordt beheerst door de bepalingen van de hoofdovereenkomst, waarbij verdere verplichtingen kunnen voortvloeien uit wettelijke bepalingen.

3. RECHTEN EN VERPLICHTINGEN VAN DE VERWERKER

3.1. De Verwerker zal de Persoonsgegevens uitsluitend verwerken op basis van de Hoofdovereenkomst, deze GVO en de gedocumenteerde instructies van de Klant - inclusief met betrekking tot de doorgifte van Persoonsgegevens naar een derde land of een internationale organisatie - tenzij de Verwerker hiertoe verplicht wordt door Unierecht of lidstatelijk recht waaraan de Verwerker onderworpen is, in welk geval de Verwerker de Klant voorafgaand aan de verwerking op de hoogte zal stellen van dergelijke wettelijke

vereisten, tenzij het betreffende recht een dergelijke kennisgeving verbiedt op grond van zwaarwegend algemeen belang.

3.2. De Verwerker garandeert dat de personen die bevoegd zijn om de persoonsgegevens te verwerken zich hebben verplicht tot geheimhouding of onderworpen zijn aan een passende wettelijke geheimhoudingsplicht.

3.3. De Verwerker neemt alle maatregelen binnen zijn invloedssfeer in overeenstemming met artikel 32 GDPR (zie de bijlage 1 bij deze GVO). Deze maatregelen zijn afhankelijk van de technische vooruitgang en de stand van de techniek. Kleine ontwikkelingen worden doorgevoerd zonder overleg met de Klant.

3.4. De Klant machtigt de Verwerker om gebruik te maken van subverwerkers (met name IT-dienstverleners). Er dient op te worden toegezien dat de subverwerker dezelfde verplichtingen aangaat die op grond van deze overeenkomst op de Verwerker rusten. Indien de subverwerker zijn verplichtingen inzake gegevensbescherming niet nakomt, is de subverwerker jegens de Klant aansprakelijk voor de nakoming van de verplichtingen van de subverwerker.

3.5. De subverwerkers die vermeld staan op https://www.concrefy.com/nl/sub-verwerkers vallen onder de algemene machtiging overeenkomstig punt 3.4

3.6. De Verwerker verbindt zich ertoe persoonsgegevens alleen buiten de Europese Economische Ruimte door te geven indien passende waarborgen zijn geboden voor de naleving van de toepasselijke wetgeving inzake gegevensbescherming (bv. sluiting van modelcontractbepalingen).

3.7. De Verwerker stelt de Klant ten minste zeven (7) dagen voorafgaand aan de inschakeling van een nieuwe of vervanging van een bestaande subverwerker op de hoogte, waarbij - uitsluitend ter beoordeling van de Verwerker - (i) een e-mail aan de Klant; of (ii) publicatie op het klantenportaal of het klantenplatform; of (iii) publicatie op https://www.concrefy.com/nl/sub-verwerkers voldoende is, en verleent de Klant hierbij het recht om bezwaar te maken tegen de inschakeling van een nieuwe of vervanging van een bestaande subVerwerker, mits deze subverwerker aantoonbaar niet hetzelfde of een redelijk vergelijkbaar beschermingsniveau voor de verwerking van persoonsgegevens waarborgt. Het bezwaar van de Klant vormt een goede reden voor de Verwerker om de overeenkomst te beëindigen in de zin van de contractuele voorwaarden. Een bezwaar van de Klant dat niet aan de bovengenoemde vereisten voldoet, is irrelevant.

3.8. Gezien de aard van de verwerking zal de Verwerker, waar mogelijk, de Klant ondersteunen met passende technische en organisatorische maatregelen om te voldoen aan zijn verplichting om te reageren op verzoeken tot uitoefening van de rechten van de betrokkene als bedoeld in Hoofdstuk III GDPR. Indien de betrokkene rechtstreeks contact opneemt met de Verwerker, zal de Verwerker deze doorverwijzen naar de Klant. Dit is op voorwaarde dat de Verwerker in staat is om de betrokkene te correleren met de Klant op basis van de door de betrokkene verstrekte informatie. De Verwerker is niet aansprakelijk in gevallen waarin de Afnemer niet volledig, correct of tijdig reageert op het verzoek van de Betrokkene.

3.9. De Verwerker zal alle persoonsgegevens volledig anonimiseren of wissen binnen een termijn van honderdtachtig (180) dagen na beëindiging van de verrichting van de verwerkingsdiensten, tenzij er een verplichting bestaat om de persoonsgegevens te bewaren op grond van het recht van de Unie of het recht van de lidstaten of de gegevens nodig zijn voor de vaststelling, uitoefening of verdediging van rechtsvorderingen.

3.10. Voorafgaand aan het anonimiseren of wissen kan de Klant de persoonsgegevens tegen vergoeding van redelijke kosten ontvangen in een door de Verwerker gekozen gangbaar elektronisch formaat.

3.11. De Verwerker zal, rekening houdend met de aard van de verwerking en de informatie waarover de Verwerker beschikt, de Klant bijstaan bij het naleven van de verplichtingen van de artikelen 32 tot en met 36 GDPR.

3.12. De Verwerker verstrekt de Klant alle informatie die nodig is om aan te tonen dat hij voldoet aan de verplichtingen uit deze GVO en voert controles uit in overeenstemming met punt 4.5 van deze GVO en draagt daaraan bij. De Klant stemt er echter mee in dat controles overeenkomstig punt 4.5 naar goeddunken van de Verwerker kunnen worden vervangen door het verstrekken van gedetailleerde

documentatie over de geïmplementeerde gegevensbeschermings- en beveiligingsmaatregelen, relevante certificeringen of verslagen van externe auditors.

3.13. De Verwerker moet de Klant onmiddellijk op de hoogte stellen als hij van mening is dat een specifieke instructie van de klant in strijd is met de toepasselijke regelgeving inzake gegevensbescherming.

4. RECHTEN EN VERPLICHTINGEN VAN DE KLANT

4.1. De Klant is als enige verantwoordelijk voor het beoordelen van de toelaatbaarheid van de opgedragen verwerking en voor het waarborgen van de rechten van betrokkenen en voor de noodzakelijke kennisgevingen aan de Verwerker. De Klant informeert de Verwerker over het contactpunt voor alle vragen die voortvloeien uit of verband houden met deze GVO.

4.2. De Klant zal alle opdrachten, deelopdrachten of instructies die afwijken van of een aanvulling vormen op de hoofdovereenkomst schriftelijk verstrekken. In dringende gevallen kunnen instructies mondeling worden gegeven. De Klant bevestigt dergelijke instructies onverwijld schriftelijk.

4.3. De Klant zal de Verwerker onmiddellijk op de hoogte brengen indien hij fouten of onregelmatigheden vaststelt bij het onderzoek van de orderresultaten.

4.4. De Klant verwerkt geen bijzondere categorieën van persoonsgegevens zonder schriftelijke toestemming van de Verwerker. De Klant zal geen gegevens verwerken van personen jonger dan 14 jaar.

4.5. Behoudens artikel 3.12 van deze GVO heeft de Klant het recht om de naleving van de in deze GVO uiteengezette verplichtingen zelf of via derden die contractueel of wettelijk tot geheimhouding verplicht zijn en die geen concurrenten zijn van de Verwerker en de aan hem gelieerde ondernemingen, ter plaatse te controleren. De Klant of een door de Klant gemachtigde derde partij zal in het kader van dergelijke controles voldoen aan de interne beveiligingsvereisten van de Verwerker (met name in overeenstemming met de toepasselijke beveiligings- en IT-richtlijnen). Omwille van vertrouwelijkheids- of veiligheidsvereisten kunnen controles ter plaatse van bepaalde omgevingen en informatie (bijvoorbeeld om de rechten van derden in gevaar te brengen of om bedrijfsgeheimen te beschermen) voor zover nodig worden beperkt. Omgevingen die niet relevant zijn voor de verplichtingen in deze GVO zijn uitdrukkelijk uitgesloten van het inzagerecht van de Klant.

4.6. De Klant draagt de kosten van deze controle. Inspecties moeten worden uitgevoerd zonder de bedrijfsvoering te verstoren en tijdens algemene kantooruren. Tenzij anders aangegeven om dringende redenen die door de Klant moeten worden gedocumenteerd, vinden de inspecties plaats na een redelijke voorafgaande kennisgeving (van ten minste 30 werkdagen), indien mogelijk gedurende maximaal één dag volgens een onderling overeengekomen schema dat de impact van de audit op de activiteiten van de Verwerker tot een minimum beperkt, en niet vaker dan om de 12 maanden.

5. SLOTBEPALINGEN

5.1. Wijzigingen van en aanvullingen op deze GVO moeten schriftelijk plaatsvinden en moeten uitdrukkelijk als zodanig worden aangeduid.

5.2. Mochten afzonderlijke bepalingen van deze GVO ongeldig of niet-afdwingbaar zijn of later ongeldig of niet-afdwingbaar worden, dan heeft dit geen invloed op de geldigheid van de rest van de Gegevensbeschermingsovereenkomst. De partijen verbinden zich ertoe een dergelijke bepaling te vervangen door een geldige. Hetzelfde geldt in het geval van een contractuele leemte.

5.3. Het Nederlandse materiële recht is van toepassing met uitsluiting van het conflictenrecht en het VN-Verdrag inzake internationale koopovereenkomsten betreffende roerende zaken.

5.4. De Duitse en Engelse taalversie van deze Verwerkersovereenkomst wordt ter informatie verstrekt. Slechts de Nederlandstalige versie is bindend tussen partijen.

Bijlage 1 -Technische en Organisatorische Maatregelen volgens Art. 32 GDPR

Vertrouwelijk (Art. 32 para. 1 lit. b GDPR)

a) Toegangscontrole

De volgende geïmplementeerde maatregelen voorkomen dat onbevoegden toegang krijgen tot faciliteiten voor gegevensverwerking:

	geïmplementeerd
Toegangscontrolesysteem, kaartlezer (magneet-/chipkaart)	✓
Deurbeveiliging (elektrische deuropener, cijferslot, enz.)	✓
Beveiligde deuren / ramen	✓
Omheiningssystemen	✓
Sleutelbeheer, documentatie van sleuteltoewijzing	✓
Fabrieksbeveiliging, portier, beveiligingsdienst	✓
Alarmsysteem	✓
Speciale beschermingsmaatregelen voor de opslag van back-ups en/of andere gegevensdragers	✓
Niet-omkeerbare vernietiging van gegevensdragers	✓
Personeels- en autorisatiebadges	✓
Afsluitbare secties	✓
Bezoekersreglement (bijv. ophalen bij receptie, documentatie van bezoekuren, bezoekersbadge, begeleiding na bezoek naar uitgang)	✓

b) Toegangscontrole

De volgende geïmplementeerde maatregelen voorkomen dat onbevoegden toegang krijgen tot gegevensverwerkingssystemen:

	geïmplementeerd
Persoonlijke en individuele gebruikerslogin bij het inloggen op het systeem of bedrijfsnetwerk	✓
Autorisatieproces voor toegangsrechten	✓
Beperking van geautoriseerde gebruikers	✓
Eenmalige aanmelding	✓
Wachtwoordbeleid (specificatie van wachtwoordparameters in termen van complexiteit en update-interval, wachtwoordgeschiedenis)	✓
Elektronische documentatie van wachtwoorden en bescherming van deze documentatie tegen onbevoegde toegang	✓
Registratie van toegang tot het systeem	✓
Extra systeemaanmelding voor bepaalde applicaties	✓
Automatische vergrendeling van clients na een bepaalde periode zonder gebruikersactiviteit (ook schermbeveiliging met wachtwoord of automatische pauze)	✓
Up-to-date firewall	✓
Bijgewerkte antivirussoftware	✓

c) Toegangscontrole

De volgende geïmplementeerde maatregelen zorgen ervoor dat onbevoegden geen toegang hebben tot persoonlijke gegevens:

	geïmplementeerd
Centraal beheer en documentatie van autorisaties	✓
Sluiting van contracten voor gegevensverwerking in opdracht voor het externe onderhoud van gegevensverwerkingssystemen, op voorwaarde dat het onderhoud op afstand de verwerking van PII inhoudt, d.w.z. de verwerking van persoonsgegevens, als onderdeel van de dienst.	✓
Autorisatieproces voor machtigingen	✓
Machtigingsroutines	✓
Profielen/rollen	
Encryptie van harde schijven en/of laptops	✓
Proces van scheiding van taken	✓
Niet-omkeerbare verwijdering van gegevensdragers	✓
Privacyschermen voor mobiele gegevensverwerkingssystemen	✓
Patchbeheer	✓

d) Controle op scheiding

De volgende maatregelen zorgen ervoor dat persoonsgegevens die voor verschillende doeleinden worden verzameld, apart worden verwerkt.

	geïmplementeerd
Opslag van gegevensrecords in afzonderlijke databases	✓
Verwerking op afzonderlijke systemen	✓
Toegangsautorisaties volgens functionele verantwoordelijkheid	✓
Multi-client mogelijkheid van IT-systemen	✓
Gebruik van testgegevens	✓
Scheiding van ontwikkel- en productieomgeving	✓
Autorisatieconcept	✓
Netwerksegmentatie	✓

Integriteit (Art. 32 para. 1 lit. b GDPR)

a) Controle op openbaarmaking

Er wordt voor gezorgd dat persoonsgegevens tijdens de overdracht of opslag op gegevensdragers niet zonder toestemming kunnen worden gelezen, gekopieerd, gewijzigd of verwijderd en dat kan worden nagegaan welke personen of instanties persoonsgegevens hebben ontvangen. De volgende maatregelen worden geïmplementeerd om dit te waarborgen:

	geïmplementeerd
Encryptie van het opslagmedium van laptops	✓
Beveiligde bestandsoverdracht (samenwerking, Sharepoint)	✓
Beveiligd gegevenstransport (bijv. TLS)	✓
Elektronische handtekening	✓
Beveiligd WLAN	✓
Regeling voor de omgang met mobiele opslagmedia (bijv. laptops, USB-stick, mobiele telefoon)	✓
Getunnelde gegevensverbindingen op afstand (VPN = Virtual Private Network)	✓
Classificatie van gegevens	✓

b) Invoercontrole

De volgende maatregelen zorgen ervoor dat het mogelijk is om te controleren wie persoonsgegevens heeft verwerkt in gegevensverwerkingssystemen en op welk moment:

	geïmplementeerd
Toegangsrechten	✓
Documentbeheersysteem (DMS) met wijzigingsgeschiedenis	✓
Functionele verantwoordelijkheden, organisatorisch gedefinieerde verantwoordelijkheden	✓

Beschikbaarheid en veerkracht (Art. 32 para. 1 lit. b GDPR)

Controle op beschikbaarheid en veerkracht

De volgende maatregelen zorgen ervoor dat persoonsgegevens worden beschermd tegen onopzettelijke vernietiging of verlies en altijd beschikbaar zijn voor de Klant:

	geïmplementeerd
Vastgestelde back-upprocedure	✓
Opslagproces voor back-ups (bijv. brandveilige kluis, apart brandcompartiment).	✓
Zorgen voor gegevensopslag in het beveiligde netwerk	✓
Beveiligingsupdates installeren als dat nodig is	✓
Spiegelen van harde schijven	✓
Installatie van een ononderbreekbare stroomvoorziening (UPS)	✓
Geschikte archiefruimte voor papieren documenten	✓
Brand- en/of bluswaterbeveiliging van de serverruimte	✓
Brand- en/of bluswaterbeveiliging van de archiefruimten	✓
Serverruimte met airconditioning	✓
Bescherming tegen virussen	✓
Firewall	✓
Redundante, lokaal gescheiden gegevensopslag (offsite opslag)	✓
Bewaking van alle relevante servers	✓
Back-up datacenter	✓
Kritische componenten zijn redundant uitgevoerd	✓

Procedure voor periodieke toetsing, beoordeling en evaluatie (Art. 32 para. 1 lit. d GDPR; Art. 25 para. 1 GDPR)

a) Beheer gegevensbescherming

De volgende maatregelen zijn bedoeld om ervoor te zorgen dat er een organisatie is die voldoet aan de basisvereisten van de gegevensbeschermingswetgeving:

	geïmplementeerd
Gegevensbeschermingsbeleid (bescherming van PII)	✓
Oprichting van een comité voor gegevensbescherming	✓
Verplichting van werknemers tot geheimhouding van gegevens	✓
Bijhouden van een overzicht van verwerkingsactiviteiten (art. 30 GDPR)	✓
Softwareoplossing voor gegevensbeschermingsbeheer in gebruik	✓
Certificering volgens ISO 9001	✓
Gestandaardiseerd proces voor het afhandelen van informatieverzoeken en andere rechten van betrokkenen	✓
Centrale documentatie van alle procedures en voorschriften voor gegevensbescherming met toegang voor medewerkers op basis van autorisatie	✓

b) Beheer van incidenten

De volgende maatregelen zijn bedoeld om ervoor te zorgen dat kennisgevingsprocessen in gang worden gezet in het geval van inbreuken op de gegevensbescherming:

	geïmplementeerd
Kennisgevingsproces voor schendingen van gegevensbescherming volgens para. 4 Nr. 12 GDPR met betrekking tot de toezichthoudende autoriteiten (art. 33 GDPR)	✓
Kennisgevingsproces voor schendingen van gegevensbescherming volgens para. 4 Nr. 12 GDPR met betrekking tot de betrokkenen (Art. 34 GDPR)	✓
Gedocumenteerde procedure voor het afhandelen van beveiligingsincidenten	✓

c) Privacyvriendelijke standaardinstellingen (Art. 25 para. 2 GDPR)

Zowel bij de gestandaardiseerde standaardinstellingen van systemen en apps als bij het instellen van gegevensverwerkingsprocedures moet rekening worden gehouden met de standaardinstellingen. In deze fase worden functies en rechten concreet geconfigureerd, wordt de toelaatbaarheid of ontoelaatbaarheid van bepaalde invoer of invoeropties (bijv. vrije teksten) gedefinieerd met betrekking tot gegevensminimalisatie en worden beslissingen genomen over de beschikbaarheid van gebruiksfuncties (bijv. met betrekking tot de omvang van de verwerking). Ook het type en de reikwijdte van de persoonlijke verwijzing of de anonimisering (bijv. in het geval van selectie-, export- en evaluatiefuncties, die standaard kunnen worden gespecificeerd en beschikbaar gesteld of vrij configureerbaar zijn) of de beschikbaarheid van bepaalde verwerkingsfuncties, logging, enz. worden gespecificeerd.

	geïmplementeerd
Invoervelden in online formulieren alleen als verplichte velden markeren als dit absoluut noodzakelijk is voor het verdere proces.	✓
Eenvoudige uitoefening van het herroepingsrecht via technische maatregelen (e-mail footer).	✓

d) Ordercontrole

De volgende maatregelen zorgen ervoor dat persoonlijke gegevens alleen volgens instructies kunnen worden verwerkt.

	geïmplementeerd
Overeenkomst van opdracht tot verwerking met voorschriften over rechten en plichten van opdrachtnemer en opdrachtgever	✓
Aanwijzing van contactpersonen en/of verantwoordelijke medewerkers	✓
Schriftelijke gegevensbeschermingsbriefing voor alle medewerkers met toegangsrechten	✓
Verplichting van alle medewerkers met toegangsrecht tot gegevens tot geheimhouding van gegevens	✓