VERWERKERSOVEREENKOMST

Candoo Repair

Versie 1.1 | 15 juni 2026

Bijlage bij de SaaS-overeenkomst / Algemene Voorwaarden Candoo Repair v1.2

Verwerker	Candoo XYZ B.V., handelend onder de handelsnaam Candoo Repair
Verwerkingsverantwoordelijke	Klant zoals aangeduid in de Hoofdovereenkomst, offerte of orderformulier
IP-eigenaar / licentiegever	Candoo Beheer B.V. (geen partij, tenzij uitdrukkelijk anders overeengekomen)

Artikel 1 – Partijen en achtergrond

1.1 Deze Verwerkersovereenkomst is van toepassing tussen de Klant als Verwerkingsverantwoordelijke en Candoo XYZ B.V., handelend onder de handelsnaam Candoo Repair, als Verwerker.

1.2 Candoo Repair is een handelsnaam van Candoo XYZ B.V., gevestigd aan Andries van Bronckhorstlaan 499, 3201 XK Spijkenisse, ingeschreven bij de Kamer van Koophandel onder nummer 94483922, met e-mailadres business@candoo.xyz.

1.3 Candoo XYZ B.V. exploiteert het Platform op basis van een licentie van Candoo Beheer B.V. Alle intellectuele eigendomsrechten op de software, broncode, architectuur, workflows, documentatie, AI-functionaliteiten, databankstructuren, prompts en overige platformtechnologie berusten bij Candoo Beheer B.V.

1.4 Candoo Beheer B.V. is geen zelfstandige contractspartij bij deze Verwerkersovereenkomst, tenzij dit uitdrukkelijk schriftelijk is overeengekomen. Voor zover Candoo Beheer B.V. in opdracht van Candoo XYZ B.V. werkzaamheden verricht waarbij Persoonsgegevens worden verwerkt, wordt zij aangemerkt als Subverwerker of onderaannemer onder verantwoordelijkheid van Candoo XYZ B.V.

1.5 Deze Verwerkersovereenkomst regelt de verwerking van Persoonsgegevens door Verwerker in het kader van de levering van het Candoo Repair Platform en aanverwante diensten aan Verwerkingsverantwoordelijke.

Artikel 2 – Definities

AI Act	Verordening (EU) 2024/1689 van het Europees Parlement en de Raad betreffende geharmoniseerde regels inzake artificiéle intelligentie.
AI-incident	Een gebeurtenis waarbij AI-functionaliteiten foutieve, ongewenste of schadelijke output produceren die betrekking heeft op Persoonsgegevens, waarbij ongeautoriseerde verwerking plaatsvindt of waarbij sprake is van een beveiligingsrisico in combinatie met AI-gebruik.
AI-provider	Een externe partij die een AI-model, foundation model of general-purpose AI-model levert dat door Verwerker wordt ingezet in het Platform.
Agent Layer	De governance-first laag voor workflow intelligence, werkzaam in OFF-, SHADOW- of LIVE-modus.

AVG	Verordening (EU) 2016/679, de Algemene Verordening Gegevensbescherming.
Algemene Voorwaarden	De Algemene Voorwaarden Candoo Repair v1.2, zoals van tijd tot tijd van toepassing.
Betrokkene	De natuurlijke persoon op wie een Persoonsgegeven betrekking heeft.
Datalek	Een inbreuk in verband met Persoonsgegevens als bedoeld in artikel 4 lid 12 AVG.
DPIA / GEB	Data Protection Impact Assessment / Gegevensbeschermingseffectbeoordeling als bedoeld in artikel 35 AVG.
Hoofdovereenkomst	De overeenkomst, offerte, orderformulier, SaaS-overeenkomst of andere afspraak op grond waarvan Candoo XYZ B.V. het Platform aan Verwerkingsverantwoordelijke levert.
Klantdata	Alle gegevens die door of namens Verwerkingsverantwoordelijke in het Platform worden ingevoerd, opgeslagen, verwerkt of verzonden.
Persoonsgegevens	Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon als bedoeld in artikel 4 lid 1 AVG.
Platform	Het Candoo Repair SaaS-platform voor reparatiebeheer, ticketbeheer, leverancierscommunicatie, klantcommunicatie, workflowondersteuning, AI-functionaliteiten, Agent Layer, externe intake, logging en aanverwante diensten.
Subverwerker	Een derde partij die door Verwerker wordt ingeschakeld voor de verwerking van Persoonsgegevens ten behoeve van Verwerkingsverantwoordelijke.
Verwerker	Candoo XYZ B.V., handelend onder de handelsnaam Candoo Repair.
Verwerkingsverantwoordelijke	De Klant die doel en middelen van de verwerking van Persoonsgegevens bepaalt.

2.1 Begrippen die niet in deze Verwerkersovereenkomst zijn gedefinieerd, hebben de betekenis die daaraan in de AVG, de Algemene Voorwaarden of de Hoofdovereenkomst wordt gegeven.

Artikel 3 – Toepasselijkheid en rangorde

3.1 Deze Verwerkersovereenkomst vormt een bijlage bij en integraal onderdeel van de Hoofdovereenkomst.

3.2 Bij strijdigheid tussen deze Verwerkersovereenkomst en de Hoofdovereenkomst geldt deze Verwerkersovereenkomst uitsluitend voor zover het de verwerking van Persoonsgegevens betreft.

3.3 Bij strijdigheid tussen deze Verwerkersovereenkomst en de Algemene Voorwaarden prevaleert deze Verwerkersovereenkomst voor privacy- en verwerkingsaangelegenheden.

3.4 De bepalingen over aansprakelijkheid, beperking van aansprakelijkheid, betaling, intellectuele eigendom, looptijd en toepasselijk recht in de Hoofdovereenkomst en Algemene Voorwaarden blijven van toepassing, tenzij in deze Verwerkersovereenkomst uitdrukkelijk anders is bepaald.

3.5 Het AI Act Addendum Candoo Repair v1.0 regelt de AI-governance, rolverdeling, intended purpose, verboden gebruik en AI-gebruiksregels. Deze Verwerkersovereenkomst regelt de privacy- en AVG-verplichtingen. Bij overlap werken partijen samen om beide verplichtingen praktisch en consistent uit te voeren.

Artikel 4 – Onderwerp, aard, doel en duur van de verwerking

4.1 Het onderwerp van de verwerking is het beschikbaar stellen, onderhouden, beveiligen, ondersteunen en doorontwikkelen van het Platform ten behoeve van Verwerkingsverantwoordelijke.

4.2 De aard van de verwerking omvat onder meer het ontvangen, vastleggen, ordenen, structureren, opslaan, wijzigen, raadplegen, gebruiken, verstrekken door middel van doorgifte, loggen, beveiligen, exporteren, wissen en vernietigen van Persoonsgegevens.

4.3 De doelen van de verwerking zijn beperkt tot de uitvoering van de Hoofdovereenkomst, waaronder:

- reparatie-intake en verwerking van service-aanvragen;
- ticketbeheer, statusopvolging en workflowcoördinatie;
- klantcommunicatie via e-mail en berichtmodule;
- leverancierscommunicatie, service-instructies en statusnotificaties;
- operationele workflowondersteuning;
- AI-ondersteunde tekstvoorstellen, samenvattingen en communicatieconcepten;
- Agent Layer workflowadvies, evaluaties en (indien geactiveerd) workflowuitvoering;
- gebruikersbeheer, rolbeheer en autorisatiebeheer;
- auditlogging, beveiligingslogging en systeemmonitoring;
- support, foutanalyse en incidentonderzoek;
- beveiliging, back-up en systeemintegriteit;

- externe intake via API of integratiekanalen;
- rapportage en operationele statistieken.

4.4 Verwerker verwerkt Persoonsgegevens gedurende de looptijd van de Hoofdovereenkomst en daarna uitsluitend voor zover noodzakelijk voor export, verwijdering, back-upretentie, wettelijke bewaarplichten of afwikkeling van openstaande verplichtingen.

4.5 De nadere omschrijving van de verwerking is opgenomen in Bijlage 1.

Artikel 5 – Rollen van partijen

5.1 Verwerkingsverantwoordelijke bepaalt het doel en de middelen van de verwerking van Persoonsgegevens binnen het Platform en is verantwoordelijk voor de rechtmatigheid van de verwerking.

5.2 Verwerker verwerkt Persoonsgegevens uitsluitend ten behoeve van Verwerkingsverantwoordelijke en uitsluitend binnen de grenzen van deze Verwerkersovereenkomst, de Hoofdovereenkomst en schriftelijke instructies van Verwerkingsverantwoordelijke.

5.3 Verwerker verwerkt Persoonsgegevens niet voor eigen zelfstandige doeleinden, behoudens voor zover gegevens volledig zijn geanonimiseerd en niet langer tot een Betrokkene herleidbaar zijn.

5.4 Indien Verwerker op grond van Unierecht of lidstatelijk recht verplicht is Persoonsgegevens te verwerken buiten de instructie van Verwerkingsverantwoordelijke, informeert Verwerker Verwerkingsverantwoordelijke daarover vooraf, tenzij de wet dit verbiedt.

Artikel 6 – Verwerking uitsluitend op instructie

6.1 Verwerker verwerkt Persoonsgegevens uitsluitend op basis van gedocumenteerde instructies van Verwerkingsverantwoordelijke.

6.2 De Hoofdovereenkomst, deze Verwerkersovereenkomst, de configuratie van het Platform, de instellingen van Verwerkingsverantwoordelijke en redelijke schriftelijke instructies van Verwerkingsverantwoordelijke gelden als gedocumenteerde instructies.

6.3 Verwerker mag een instructie weigeren of opschorten indien Verwerker redelijkerwijs meent dat uitvoering daarvan in strijd is met de AVG, andere toepasselijke wetgeving, de AI Act, beveiligingsvereisten, rechten van derden of de Hoofdovereenkomst. Verwerker stelt Verwerkingsverantwoordelijke hiervan op de hoogte, voor zover toegestaan.

6.4 Verwerker is niet gehouden instructies uit te voeren die buiten de overeengekomen dienstverlening vallen, tenzij partijen daarover aanvullende afspraken maken.

Artikel 7 – Verplichtingen van Verwerkingsverantwoordelijke

7.1 Verwerkingsverantwoordelijke garandeert dat zij voor alle verwerkingen binnen het Platform beschikt over een geldige rechtsgrond onder de AVG.

7.2 Verwerkingsverantwoordelijke is verantwoordelijk voor het informeren van Betrokkenen over de verwerking, waaronder eindklanten, medewerkers, leverancierscontactpersonen en eventuele reparateurs of servicepartners.

7.3 Verwerkingsverantwoordelijke is verantwoordelijk voor de juistheid, volledigheid, proportionaliteit en noodzakelijkheid van de in het Platform ingevoerde Persoonsgegevens.

7.4 Verwerkingsverantwoordelijke zal geen bijzondere categorieën persoonsgegevens, strafrechtelijke gegevens, BSN-nummers, betaalkaartgegevens of andere zeer gevoelige gegevens in het Platform invoeren, tenzij dit noodzakelijk is voor de eigen dienstverlening en Verwerkingsverantwoordelijke daarvoor zelf een geldige wettelijke grondslag en passende waarborgen heeft.

7.5 Verwerkingsverantwoordelijke zal vermijden dat onnodige bijzondere persoonsgegevens, onnodig gedetailleerde persoonsgegevens of persoonsgegevens van betrokkenen waarvoor geen rechtsgrond bestaat, in vrije tekstvelden, prompts of AI-invoer worden ingevoerd.

7.6 Verwerkingsverantwoordelijke is verantwoordelijk voor het beheer van gebruikersaccounts, rollen, autorisaties en de intrekking van toegang van eigen medewerkers of andere Gebruikers.

7.7 Verwerkingsverantwoordelijke meldt beveiligingsincidenten, misconfiguraties, ongewenste AI-output met persoonsgegevens en onrechtmatige invoer door eigen gebruikers die zij zelf constateert onverwijld aan Verwerker.

Artikel 8 – Verplichtingen van Verwerker

8.1 Verwerker verwerkt Persoonsgegevens zorgvuldig, behoorlijk en in overeenstemming met deze Verwerkersovereenkomst.

8.2 Verwerker neemt passende technische en organisatorische maatregelen als bedoeld in artikel 32 AVG, rekening houdend met de stand van de techniek, uitvoeringskosten, aard, omvang, context en doeleinden van de verwerking en de risico's voor Betrokkenen.

8.3 Verwerker verleent redelijke medewerking aan Verwerkingsverantwoordelijke bij het nakomen van diens AVG-verplichtingen, voor zover deze medewerking redelijkerwijs binnen de invloedssfeer van Verwerker ligt.

8.4 Verwerker zorgt ervoor dat medewerkers en hulppersonen die toegang hebben tot Persoonsgegevens gebonden zijn aan geheimhouding of een passende wettelijke verplichting tot vertrouwelijkheid.

8.5 Verwerker houdt, voor zover vereist, een register bij van verwerkingsactiviteiten waarvoor Verwerker verantwoordelijk is als verwerker.

Artikel 9 – Vertrouwelijkheid

9.1 Verwerker houdt alle Persoonsgegevens en Klantdata vertrouwelijk en gebruikt deze uitsluitend voor de uitvoering van de Hoofdovereenkomst.

9.2 Toegang tot Persoonsgegevens wordt beperkt tot personen voor wie toegang noodzakelijk is voor levering, support, beveiliging, onderhoud of beheer van het Platform (least privilege).

9.3 De geheimhoudingsverplichting blijft ook na beëindiging van de Hoofdovereenkomst en deze Verwerkersovereenkomst van kracht.

Artikel 10 – Beveiliging en technische maatregelen

10.1 Verwerker treft passende technische en organisatorische maatregelen om Persoonsgegevens te beschermen tegen verlies, ongeoorloofde toegang, onbevoegde wijziging, ongeoorloofde openbaarmaking en onrechtmatige verwerking.

10.2 De maatregelen omvatten, afhankelijk van de functionaliteit en technische beschikbaarheid, onder meer: toegangsbeveiliging, rolgebaseerde autorisatie, least privilege, logging, tenant-isolatie, versleuteling van transport en opslag waar passend, back-ups, beveiligd transport, scheiding van omgevingen, incidentrespons, bescherming van secrets en API-sleutels, en beperking van supporttoegang.

10.3 Een overzicht van de belangrijkste technische en organisatorische maatregelen is opgenomen in Bijlage 3.

10.4 Verwerker mag beveiligingsmaatregelen aanpassen indien dit noodzakelijk of wenselijk is voor verbetering van beveiliging, schaalbaarheid, onderhoudbaarheid of compliance, mits het algemene beveiligingsniveau niet wezenlijk wordt verlaagd.

Artikel 11 – Multi-tenant gegevensscheiding

11.1 Het Platform is ingericht als multi-tenant SaaS-omgeving. Gegevens van verschillende klanten worden logisch van elkaar gescheiden.

11.2 Verwerker past tenant-scoping, autorisaties, server-side controles en waar passend databasebeveiliging toe om te voorkomen dat klanten toegang krijgen tot gegevens van andere klanten.

11.3 Tenzij uitdrukkelijk schriftelijk anders overeengekomen, heeft Verwerkingsverantwoordelijke geen recht op een fysiek gescheiden database, dedicated hostingomgeving of afzonderlijke applicatie-instantie.

11.4 Verwerker mag geaggregeerde, geanonimiseerde en niet-herleidbare statistieken gebruiken voor beveiliging, capaciteitsplanning, productverbetering, rapportage en strategische analyse.

Artikel 12 – Subverwerkers

12.1 Verwerkingsverantwoordelijke verleent Verwerker algemene toestemming om Subverwerkers in te schakelen voor de uitvoering van de Hoofdovereenkomst, met inbegrip van cloudhosting, databasehosting, e-mailproviders, AI-providers, monitoring- en loggingdiensten, support-tooling en Candoo Beheer B.V. voor zover zij toegang heeft tot Persoonsgegevens.

12.2 Verwerker houdt een actueel overzicht bij van Subverwerkers of stelt dit op verzoek beschikbaar. Een initieel overzicht is opgenomen in Bijlage 4.

12.3 Verwerker legt aan Subverwerkers verplichtingen op die, voor zover relevant, ten minste een vergelijkbaar beschermingsniveau bieden als deze Verwerkersovereenkomst.

12.4 Verwerker informeert Verwerkingsverantwoordelijke over wezenlijke wijzigingen in Subverwerkers via e-mail, platformmelding, release notes of een online subverwerkersregister.

12.5 Verwerkingsverantwoordelijke kan binnen veertien (14) dagen na kennisgeving schriftelijk en gemotiveerd bezwaar maken tegen een nieuwe Subverwerker indien sprake is van concrete privacy- of beveiligingsrisico's. Partijen treden in overleg over een redelijke oplossing.

12.6 Indien geen redelijke oplossing mogelijk is en de betreffende Subverwerker noodzakelijk is voor de dienstverlening, kan Verwerker de betreffende functionaliteit beperken of de Hoofdovereenkomst beëindigen met inachtneming van een redelijke termijn.

Artikel 13 – Doorgifte buiten de Europese Economische Ruimte

13.1 Verwerker verwerkt Persoonsgegevens bij voorkeur binnen de Europese Economische Ruimte, voor zover dit redelijkerwijs mogelijk is binnen de gekozen hosting-, AI-, e-mail- en infrastructuurdiensten.

13.2 Indien Persoonsgegevens worden doorgegeven aan landen buiten de Europese Economische Ruimte waarvoor geen adequaatheidsbesluit geldt, zorgt Verwerker voor passende waarborgen, zoals standaardcontractbepalingen van de Europese Commissie of een ander geldig doorgiftemechanisme.

13.3 Verwerker mag doorgiften uitvoeren voor zover deze noodzakelijk zijn voor de levering van functionaliteiten die door Verwerkingsverantwoordelijke zijn geactiveerd, waaronder AI-functionaliteiten, e-mailverzending, hosting, monitoring of support.

13.4 Verwerkingsverantwoordelijke erkent dat externe diensten, zoals AI-providers en e-mailproviders, eigen verwerkingslocaties kunnen hanteren. De relevante Subverwerkers en locaties worden zo veel mogelijk in Bijlage 4 opgenomen of op verzoek verstrekt.

Artikel 14 – Datalekken en beveiligingsincidenten

14.1 Verwerker maakt onderscheid tussen:

- een AVG-Datalek: een inbreuk in verband met Persoonsgegevens als bedoeld in artikel 4 lid 12 AVG;

- een beveiligingsincident: een incident waarbij de vertrouwelijkheid, integriteit of beschikbaarheid van systemen of gegevens in gevaar is, ongeacht of dit Persoonsgegevens betreft;
- een AI-incident met Persoonsgegevens: ongewenste of foutieve verwerking van Persoonsgegevens door AI-functionaliteiten, ongeautoriseerde output met Persoonsgegevens, of beveiligingsrisico door AI-gebruik.

14.2 Verwerker informeert Verwerkingsverantwoordelijke zonder onredelijke vertraging nadat Verwerker kennis heeft genomen van een Datalek of een AI-incident met Persoonsgegevens dat betrekking heeft op gegevens van Verwerkingsverantwoordelijke.

14.3 Verwerker streeft ernaar een melding aan Verwerkingsverantwoordelijke uiterlijk binnen achtenveertig (48) uur na ontdekking te doen, voor zover dit redelijkerwijs mogelijk is gelet op de aard van het incident en de beschikbare informatie.

14.4 De melding bevat, voor zover bekend en relevant: de aard van het incident, de getroffen Persoonsgegevens, de betrokken systemen, de waarschijnlijke gevolgen, reeds genomen maatregelen en contactgegevens voor opvolging.

14.5 Verwerkingsverantwoordelijke blijft zelf verantwoordelijk voor eventuele meldingen aan de Autoriteit Persoonsgegevens en/of Betrokkenen. SLA-responstijden van Verwerker zijn niet automatisch gelijkgesteld aan wettelijke meldtermijnen voor Verwerkingsverantwoordelijke.

14.6 Verwerker verleent redelijke medewerking aan onderzoek en opvolging van het Datalek of AI-incident. De procedure is nader uitgewerkt in Bijlage 6.

Artikel 15 – Rechten van betrokkenen

15.1 Voor zover een Betrokkene een verzoek rechtstreeks bij Verwerker indient, zal Verwerker dit verzoek doorsturen aan Verwerkingsverantwoordelijke, tenzij Verwerker wettelijk verplicht is zelfstandig te reageren.

15.2 Verwerker verleent, voor zover mogelijk en redelijk, bijstand aan Verwerkingsverantwoordelijke bij verzoeken tot inzage, rectificatie, verwijdering, beperking, dataportabiliteit en bezwaar.

15.3 Verwerker reageert niet zelfstandig inhoudelijk op verzoeken van Betrokkenen. De inhoudelijke beoordeling en communicatie met Betrokkenen berust bij Verwerkingsverantwoordelijke.

15.4 Klant blijft verantwoordelijk voor tijdige communicatie met Betrokkenen over hun rechten en de afhandeling van hun verzoeken.

15.5 Indien voor de afhandeling van verzoeken aanvullende technische of handmatige werkzaamheden nodig zijn buiten de standaardfunctionaliteit van het Platform, mag Verwerker daarvoor redelijke kosten in rekening brengen.

Artikel 16 – Bijstand bij AVG-verplichtingen en DPIA

16.1 Verwerker verleent redelijke bijstand aan Verwerkingsverantwoordelijke bij het nakomen van verplichtingen op grond van de artikelen 32 tot en met 36 AVG, voor zover deze betrekking hebben op de verwerking door Verwerker.

16.2 Deze bijstand kan onder meer bestaan uit het verstrekken van informatie over beveiligingsmaatregelen, subverwerkers, datalekken, technische mogelijkheden voor dataverwijdering of export en relevante systeeminformatie.

16.3 Verwerkingsverantwoordelijke is zelf verantwoordelijk voor de beoordeling of een DPIA of GEB vereist is op grond van artikel 35 AVG, gelet op de aard, omvang, context en doeleinden van de verwerking.

16.4 Verwerker verstrekt op redelijk verzoek informatie over de verwerking, beveiligingsmaatregelen, subverwerkers en technische architectuur ter ondersteuning van een DPIA door Verwerkingsverantwoordelijke.

16.5 Verwerker is niet gehouden om juridische adviezen te geven of DPIA's op te stellen namens Verwerkingsverantwoordelijke. Omvangrijke bijstand bij DPIA-ondersteuning kan afzonderlijk in rekening worden gebracht, tenzij het verzoek voortvloeit uit een aantoonbare tekortkoming van Verwerker.

Artikel 17 – Audit en informatieverstrekking

17.1 Verwerker stelt Verwerkingsverantwoordelijke op redelijk verzoek informatie ter beschikking die nodig is om naleving van deze Verwerkersovereenkomst aan te tonen.

17.2 Verwerkingsverantwoordelijke mag maximaal eenmaal per kalenderjaar een audit laten uitvoeren, tenzij sprake is van een concreet en ernstig beveiligingsincident dat een aanvullende audit redelijkerwijs noodzakelijk maakt.

17.3 Een audit vindt plaats na ten minste twintig (20) werkdagen voorafgaande schriftelijke kennisgeving, tijdens normale kantooruren en op zodanige wijze dat de bedrijfsvoering, beveiliging, vertrouwelijkheid en rechten van andere klanten niet worden geschaad.

17.4 Verwerker mag verlangen dat een audit wordt uitgevoerd door een onafhankelijke deskundige die aan passende geheimhouding is gebonden.

17.5 Audits geven geen recht op toegang tot broncode, bedrijfsgeheimen, gegevens van andere klanten, beveiligingsgevoelige details of systemen van Subverwerkers buiten de contractuele mogelijkheden van Verwerker.

17.6 Indien Verwerker beschikt over relevante certificeringen, auditrapporten, pen-testverklaringen of security summaries, mag Verwerker deze verstrekken als alternatief voor of onderdeel van de audit.

Artikel 18 – Teruggave en verwijdering van gegevens

18.1 Na beëindiging van de Hoofdovereenkomst stelt Verwerker Verwerkingsverantwoordelijke gedurende dertig (30) dagen in de gelegenheid om Klantdata te exporteren, tenzij partijen schriftelijk een andere termijn overeenkomen.

18.2 Na afloop van de exporttermijn mag Verwerker Persoonsgegevens uit actieve systemen verwijderen, tenzij wettelijke bewaarplichten, openstaande geschillen, beveiligingsredenen of overeengekomen bewaartermijnen verdere opslag rechtvaardigen.

18.3 Persoonsgegevens kunnen tijdelijk aanwezig blijven in back-ups, logbestanden en technische archieven totdat deze volgens het reguliere retentiebeleid worden overschreven of verwijderd.

18.4 Geanonimiseerde en geaggregeerde statistieken die niet meer herleidbaar zijn tot Betrokkenen of Verwerkingsverantwoordelijke mogen worden bewaard voor beveiliging, capaciteitsplanning en analyse.

18.5 Nadere bewaartermijnen zijn opgenomen in Bijlage 5.

Artikel 19 – AI-functionaliteiten en verwerking van persoonsgegevens

19.1 Het Platform kan AI-functionaliteiten bevatten voor onder meer tekstvoorstellen, communicatieconcepten, workflowadviezen, samenvattingen, classificaties of andere ondersteunende functies. Voor zover AI-functionaliteiten Persoonsgegevens verwerken, vindt die verwerking plaats ten behoeve van Verwerkingsverantwoordelijke en binnen de grenzen van de Hoofdovereenkomst, deze Verwerkersovereenkomst en de door Verwerkingsverantwoordelijke geactiveerde instellingen.

19.2 AI-functionaliteiten zijn ondersteunend van aard. Zij nemen geen zelfstandige juridische, financiële of operationele besluiten namens Verwerkingsverantwoordelijke. Verwerkingsverantwoordelijke blijft verantwoordelijk voor controle, goedkeuring en gebruik van AI-output, inclusief de vraag of AI-output aan Betrokkenen, leveranciers of derden wordt verzonden.

19.3 Verwerkingsverantwoordelijke is verantwoordelijk voor de rechtmatigheid van Persoonsgegevens die worden ingevoerd in vrije tekstvelden, prompts, templates of andere AI-invoer. Verwerkingsverantwoordelijke zal vermijden dat bijzondere persoonsgegevens of persoonsgegevens waarvoor geen rechtsgrond bestaat in de AI-invoer worden opgenomen.

19.4 Verwerker gebruikt Persoonsgegevens van Verwerkingsverantwoordelijke niet doelbewust voor het trainen van algemene AI-modellen van Verwerker of derden, tenzij Verwerkingsverantwoordelijke daarvoor vooraf schriftelijk toestemming heeft gegeven. Dit laat het gebruik van volledig geanonimiseerde en niet-herleidbare gegevens onverlet.

19.5 Externe AI-providers mogen Persoonsgegevens van Verwerkingsverantwoordelijke niet gebruiken voor training van algemene AI-modellen voor zover Verwerker dit contractueel of technisch kan afdwingen via gekozen zakelijke of API-instellingen. Indien een providerbeleid wijzigt, mag Verwerker de provider of instellingen aanpassen.

19.6 Indien Verwerkingsverantwoordelijke AI-functionaliteiten activeert waarbij Persoonsgegevens worden verwerkt door een externe AI-provider, geldt die AI-provider als Subverwerker voor zover zij Persoonsgegevens namens Verwerker verwerkt.

19.7 Verwerker mag AI-functionaliteiten tijdelijk beperken, uitschakelen of aanpassen indien dit noodzakelijk is vanwege beveiliging, privacy, wetgeving, providerbeperkingen, misbruik, kwaliteit of compliance-risico's.

Artikel 20 – Agent Layer en geautomatiseerde werkstromen

20.1 De Agent Layer verwerkt uitsluitend Persoonsgegevens in de modus die door Verwerkingsverantwoordelijke is geconfigureerd (OFF, SHADOW of LIVE).

20.2 In SHADOW-modus worden geen uitvoeringsacties gegenereerd of berichten verzonden.

20.3 In LIVE-modus kunnen, voor zover geactiveerd en contractueel beschikbaar, acties worden uitgevoerd die Persoonsgegevens raken, zoals het verzenden van communicatie. Verwerkingsverantwoordelijke aanvaardt daarmee de verwerkingsverantwoordelijkheid voor de inhoud van die berichten.

20.4 Verwerker mag de Agent Layer tijdelijk terugzetten naar SHADOW of OFF bij beveiligingsrisico, AI-incident, compliance-risico of onjuiste configuratie.

Artikel 21 – Logs, audittrail en supporttoegang

21.1 Het Platform legt systeemlogs, ticket events, auditlogs, communicatie-events, queue-events, foutmeldingen, toegangslogs en andere metadata vast voor beveiliging, support, foutanalyse, compliance, operationele administratie en geschilafhandeling.

21.2 Logs kunnen Persoonsgegevens bevatten, zoals gebruikersidentificatoren, e-mailadressen, ticketnummers, IP-adressen, tijdstempels, eventinformatie en berichtmetadata.

21.3 Bewaartermijnen voor logs zijn opgenomen in Bijlage 5 of gemarkeerd als [INVULLEN] ter invulling door Verwerkingsverantwoordelijke in overleg met Verwerker.

21.4 Supportmedewerkers van Verwerker krijgen uitsluitend toegang tot Klantdata voor zover noodzakelijk voor ondersteuning, probleemoplossing, beveiliging, onderhoud of wettelijke verplichtingen (least privilege).

21.5 Verwerker mag platformlogs gebruiken als operationele administratie en bewijs van uitgevoerde systeemhandelingen.

Artikel 22 – Geheimhouding en bedrijfsvertrouwelijke informatie

22.1 Persoonsgegevens, Klantdata, configuraties, API-sleutels, integratiegegevens, prompts, templates, communicatie-inhoud en bedrijfsinformatie van Verwerkingsverantwoordelijke worden als vertrouwelijk behandeld.

22.2 Verwerkingsverantwoordelijke behandelt op haar beurt informatie over de beveiliging, architectuur, broncode, infrastructuur, licenties, tarieven, roadmaps en interne werking van het Platform als vertrouwelijk.

22.3 Deze geheimhoudingsverplichtingen gelden niet voor informatie die reeds publiek bekend is zonder schending van een verplichting, rechtmatig van een derde is verkregen of op grond van wet- of regelgeving moet worden verstrekt.

Artikel 23 – Aansprakelijkheid en vrijwaring

23.1 De aansprakelijkheid van Verwerker onder deze Verwerkersovereenkomst is beperkt overeenkomstig de aansprakelijkheidsbepalingen in de Hoofdovereenkomst en de Algemene Voorwaarden.

23.2 Deze Verwerkersovereenkomst vergroot of wijzigt de aansprakelijkheidsbeperkingen uit de Hoofdovereenkomst niet, tenzij dwingend recht anders bepaalt.

23.3 Verwerkingsverantwoordelijke vrijwaart Verwerker, Candoo Beheer B.V., hun bestuurders, medewerkers, hulppersonen en Subverwerkers tegen aanspraken van derden die voortvloeien uit: onrechtmatige instructies; onjuiste of onvolledige informatie; ontbreken van een rechtsgrond; onrechtmatige inhoud; onjuiste communicatie; invoer van bijzondere persoonsgegevens zonder rechtsgrond; of ander handelen of nalaten van Verwerkingsverantwoordelijke of haar Gebruikers.

23.4 Verwerker is niet aansprakelijk voor schade die voortvloeit uit door Verwerkingsverantwoordelijke ingevoerde gegevens, verzonden communicatie, foutieve configuratie, gebruik van externe integraties of beslissingen op basis van AI-output zonder menselijke controle.

Artikel 24 – Duur en einde

24.1 Deze Verwerkersovereenkomst treedt in werking op het moment waarop de Hoofdovereenkomst tot stand komt of op het moment waarop Verwerker voor het eerst Persoonsgegevens namens Verwerkingsverantwoordelijke verwerkt.

24.2 Deze Verwerkersovereenkomst blijft van kracht zolang Verwerker Persoonsgegevens namens Verwerkingsverantwoordelijke verwerkt.

24.3 Bepalingen die naar hun aard bedoeld zijn om na beëindiging voort te duren, waaronder geheimhouding, audit voor zover relevant, aansprakelijkheid, verwijdering, bewijslast, vrijwaring en toepasselijk recht, blijven na beëindiging van kracht.

Artikel 25 – Wijzigingen

25.1 Verwerker mag deze Verwerkersovereenkomst wijzigen indien dit noodzakelijk is vanwege gewijzigde wetgeving (waaronder de AI Act), gewijzigde dienstverlening, nieuwe functionaliteiten, gewijzigde Subverwerkers, beveiligingsmaatregelen of redelijke operationele belangen.

25.2 Materiële wijzigingen worden vooraf aan Verwerkingsverantwoordelijke bekendgemaakt, tenzij de wijziging direct noodzakelijk is vanwege beveiliging, compliance of wettelijke verplichtingen.

25.3 Indien Verwerkingsverantwoordelijke redelijkerwijs niet kan instemmen met een materiële wijziging die wezenlijk nadelig is voor de bescherming van Persoonsgegevens, treden partijen in overleg over een passende oplossing.

Artikel 26 – Toepasselijk recht en geschillen

26.1 Op deze Verwerkersovereenkomst is Nederlands recht van toepassing.

26.2 Geschillen worden beslecht overeenkomstig de geschillenregeling in de Hoofdovereenkomst of Algemene Voorwaarden.

26.3 Voor zover dwingendrechtelijke privacyregels anders bepalen, blijven deze regels onverkort van toepassing.

Bijlage 1 – Omschrijving van de verwerking

Onderwerp	Beschikbaarstelling, onderhoud, beveiliging, support en doorontwikkeling van het Candoo Repair Platform.
Aard van de verwerking	Ontvangen, vastleggen, opslaan, structureren, wijzigen, raadplegen, gebruiken, verzenden, loggen, analyseren, exporteren, verwijderen en beveiligen van Persoonsgegevens.
Doeleinden	Reparatie-intake, ticketbeheer, statusopvolging, klantcommunicatie, leverancierscommunicatie, interne notities, workflowadvies, AI-ondersteunde communicatieconcepten, Agent Layer workflowadvies, auditlogging, gebruikersbeheer, support, beveiliging, back-up, externe intake, systeemmonitoring en rapportage.
Systemen/modules	Retailer portal, ticket engine, locaties/merkenconfiguratie, attachments, outbound mail queue, message templates, AI communication layer, Agent Layer (workflow intelligence), audit logs, externe intake/API, integraties en gebruikersbeheer.
Duur	Looptijd van de Hoofdovereenkomst plus de periode die nodig is voor export, verwijdering, back-upretentie of wettelijke bewaarplicht.
Frequentie	Doorlopend, afhankelijk van gebruik door Verwerkingsverantwoordelijke en haar Gebruikers.

Bijlage 2 – Categorieën persoonsgegevens en betrokkenen

Categorie Betrokkene	Mogelijke Persoonsgegevens
Eindklanten / consumenten	Naam, e-mailadres, telefoonnummer, ordernummer, ticketnummer, product- en merkgegevens, probleemomschrijving, reparatiegegevens, reparatiestatus, correspondentie, bijlagen (foto's, aankoopbewijzen, documenten), locatie-/vestigingsinformatie, communicatiehistorie en eventuele persoonsgegevens in vrije tekstvelden.
Medewerkers / Gebruikers van Verwerkingsverantwoordelijke	Naam, e-mailadres, rol, autorisaties, login-/accountgegevens, auditlogs, handelingen in het Platform, tijdstempels, supportcommunicatie en logging-metadata.
Leverancierscontactpersonen	Naam, zakelijk e-mailadres, telefoonnummer, bedrijfsnaam, rol/functie, correspondentie, service-instructies, statusupdates en communicatiehistorie.
Reparateurs / servicepartners	Naam, bedrijfsnaam, contactgegevens, statusupdates, claim-/werkorderinformatie, communicatiehistorie en operationele metadata.
Overige contactpersonen	Gegevens die incidenteel voorkomen in notities, e-mails, bijlagen, ticketomschrijving, vrije tekstvelden, prompts of supportverzoeken.

Bijzondere categorieën persoonsgegevens, strafrechtelijke gegevens, BSN-nummers, medische gegevens en betaalkaartgegevens zijn niet bedoeld voor verwerking binnen het Platform, tenzij Verwerkingsverantwoordelijke daarvoor zelf een geldige grondslag en passende maatregelen heeft.

Bijlage 3 – Technische en organisatorische maatregelen

Maatregel	Omschrijving
Toegangsbeheer	Gebruikersaccounts, rolgebaseerde autorisaties, tenant-scoping, server-side toegangscontroles, least privilege voor medewerkers en subverwerkers.
Tenant-isolatie	Logische scheiding per retailer/tenant, scoped queries, server-side guards en waar passend database policies voor scheiding van Klantdata.
Transportbeveiliging	Gebruik van beveiligde verbindingen (TLS/HTTPS) voor toegang tot het Platform en API-verkeer, voor zover technisch beschikbaar en passend.
Opslagbeveiliging	Beveiligde hosting- en databaseomgeving, toegang beperkt tot bevoegde systemen en medewerkers, gebruik van encryptie at rest en in transit waar passend.
Logging en audittrail	Vastleggen van relevante systeemhandelingen, ticket events, queue-events, statuswijzigingen, foutmeldingen, toegangslogs en supportacties voor beveiliging en compliance. Bewaartermijnen conform Bijlage 5.
Back-ups en herstel	Reguliere back-up- en herstelmaatregelen volgens het technische beleid van de hosting- en databaseomgeving. Back-ups zijn geen toegangskanaal voor Klantdata-export.
Incidentrespons	Procedure voor signalering, beoordeling, opvolging en melding van beveiligingsincidenten, Datalekken en AI-incidenten. Melding aan Verwerkingsverantwoordelijke conform artikel 14.
Geheimhouding	Vertrouwelijkheidsverplichtingen voor medewerkers en hulppersonen die toegang kunnen hebben tot Persoonsgegevens.
Subverwerkersbeheer	Contractuele verplichtingen met Subverwerkers, periodieke herbeoordeling en informatievoorziening aan Verwerkingsverantwoordelijke.

AI-beheersing	AI-functionaliteiten zijn configureerbaar en ondersteunend. Persoonsgegevens worden niet gebruikt voor training van algemene AI-modellen zonder voorafgaande schriftelijke toestemming. AI-providers worden als Subverwerker opgenomen voor zover zij Persoonsgegevens verwerken.
API- en secretbeheer	API keys, intake keys en secrets worden server-side beheerd en mogen niet in frontendcode of publieke documentatie worden opgenomen.
Beperking supporttoegang	Supporttoegang tot Klantdata vindt alleen plaats wanneer dit noodzakelijk is voor support, beveiliging, onderhoud of wettelijke verplichtingen (least privilege). Acties worden gelogd.
Scheiding van omgevingen	Productie-, test- en ontwikkelomgevingen worden logisch of fysiek van elkaar gescheiden, voor zover technisch en operationeel realiseerbaar.

Bijlage 4 – Subverwerkersregister

Subverwerker	Dienst	Gegevenscategorieën	Locatie	Waarborg
Supabase / database- en auth-provider	Database, authenticatie, storage en backend-infrastructuur	Ticketdata, gebruikersdata, logs, bijlagen	EER/VS of conform providerinstellingen	DPA/SCCs; exacte entiteit en locatie controleren
Vercel, Cloudflare of hosting/CDN-provider	Hosting, applicatie-infrastructuur, CDN, beveiliging	Technische logs, IP-adressen, requestdata, applicatiedata	EER/wereldwijd afhankelijk van provider	DPA/SCCs; exacte provider invullen
MailerSend, Resend of SMTP-provider	Verzending van klant- en leverancierscommunicatie	E-mailadressen, onderwerp, inhoud, metadata, statusinformatie	Afhankelijk van provider	DPA/SCCs; actieve provider invullen
OpenAI, Anthropic of andere AI-provider	AI-tekstvoorstellen, samenvattingen, classificaties, workflowondersteuning	Promptdata, ticketcontext, conceptteksten, metadata	Afhankelijk van provider	AI-training uitsluiten waar mogelijk; DPA/SCCs; zakelijke API-instellingen controleren
Monitoring/logging provider [nog i.o.]	Foutanalyse, performance, beveiliging en incidentonderzoek	Technische logs, gebruikers-ID's, IP-adressen, foutmeldingen	Afhankelijk van provider	Alleen indien actief; privacy-instellingen beperken
Support-tooling [nog i.o.]	Interne supportcommunicatie en ticketopvolging	Alleen gegevens die noodzakelijk zijn voor support	EER/afhankelijk van provider	Beperkt tot noodzakelijke gegevens; DPA indien vereist
Candoo Beheer B.V.	Ondersteuning namens Verwerker	Alleen gegevens die noodzakelijk zijn voor het oplossen van issues	Nederland/EER	least privilege; geheimhoudingsplicht

Bijlage 5 – Bewaartermijnen en verwijdering

Gegevenstype	Bewaartermijn / verwijdering
Actieve ticket- en klantdata	Gedurende de looptijd van de Hoofdovereenkomst, tenzij Verwerkingsverantwoordelijke eerder verwijdert of een andere termijn configureert.
Ticket events en auditlogs	Gedurende de looptijd en eventueel langer indien noodzakelijk voor beveiliging, compliance, geschilafhandeling of wettelijke verplichtingen. Standaardtermijn nader te configureren of 12 maanden na looptijd.
Systeem- en toegangslogs	Maximaal 24 maanden na vastlegging, tenzij een beveiligingsincident of wettelijke verplichting langere bewaring vereist.
AI-log / prompthistorie	Zolang noodzakelijk voor beveiliging, foutanalyse en compliance. Standaardtermijn 24 maanden; geen bewaring voor AI-training.
Outbound mail queue en communicatie-events	Gedurende de looptijd of zolang noodzakelijk voor operationele administratie, bewijs, support en foutanalyse.
Back-ups	Volgens reguliere back-upcyclus. Back-ups kunnen tijdelijk Persoonsgegevens bevatten na verwijdering uit actieve systemen. Richttermijn: maximaal 90 dagen, tenzij providerbeleid of wettelijke verplichtingen anders vereisen.
Supporttickets en correspondentie	Zolang noodzakelijk voor support, bewijs, facturatie, compliance of geschilafhandeling.
Data-export na beëindiging	Beschikbaar gedurende 30 dagen na beëindiging, tenzij schriftelijk anders overeengekomen.
Geanonimiseerde statistieken	Mogen worden bewaard zolang zij niet meer herleidbaar zijn tot Betrokkenen of Verwerkingsverantwoordelijke.

Bijlage 6 – Datalekprocedure

Stap	Omschrijving
1. Signalering	Verwerker registreert en beoordeelt signalen van mogelijke beveiligingsincidenten, Datalekken of AI-incidenten met Persoonsgegevens.
2. Eerste beoordeling	Verwerker beoordeelt of sprake kan zijn van verlies, ongeoorloofde toegang, wijziging, openbaarmaking of onrechtmatige verwerking van Persoonsgegevens, inclusief via AI-functionaliteiten.
3. Melding aan Verwerkingsverantwoordelijke	Indien een Datalek of AI-incident betrekking kan hebben op Persoonsgegevens van Verwerkingsverantwoordelijke, informeert Verwerker Verwerkingsverantwoordelijke zonder onredelijke vertraging en streeft Verwerker naar melding binnen 48 uur na ontdekking.
4. Informatievoorziening	Verwerker verstrekt beschikbare informatie over aard, omvang, categorieën gegevens, vermoedelijke gevolgen en genomen of voorgestelde maatregelen.
5. Beheersmaatregelen	Verwerker neemt redelijke technische en organisatorische maatregelen om het incident te beperken, te onderzoeken en herhaling te voorkomen. Bij AI-incidenten kan Verwerker AI-functionaliteiten tijdelijk beperken.
6. Verantwoordelijkheid melding toezichthouder	Verwerkingsverantwoordelijke beoordeelt of melding aan de Autoriteit Persoonsgegevens of Betrokkenen vereist is en blijft daarvoor verantwoordelijk. SLA-termijnen van Verwerker gelden niet als wettelijke meldtermijnen voor Verwerkingsverantwoordelijke.
7. Evaluatie	Partijen werken redelijkerwijs mee aan evaluatie en verbetering na een Datalek of AI-incident, binnen de grenzen van hun rol en verantwoordelijkheid.