

BELCO

Belco Verwerkersovereenkomst

Data Processing Agreement versie 2.0

STATUS	Publicatieversie
VERSIE	2.0
PUBLICATIEDATUM	29 september 2026
NIEUWE KLANTEN	Na elektronische acceptatie op of na 29 september 2026
BESTAANDE KLANTEN	Na elektronische acceptatie van versie 2.0 in Belco
TALEN	Nederlands en Engels
DOCUMENT ID	BELCO-DPA-2.0-2026-09-29

Deze publicatie bevat de volledige Nederlandse en Engelse tekst. Bij verschil in uitleg is de Nederlandse tekst leidend.

Nederlandse tekst

De Nederlandse tekst is leidend bij verschil in uitleg.

Partijen

Deze verwerkersovereenkomst (de “**Verwerkersovereenkomst**”) wordt gesloten tussen:

1. de rechtspersoon of natuurlijke persoon handelend in de uitoefening van een beroep of bedrijf voor wie een Belco-organisatieaccount is geopend of die een abonnement op de Dienst afneemt, zoals met organisatienaam en factuurgegevens in Belco geregistreerd (de “**Klant**” of “**Verwerkingsverantwoordelijke**”); en
2. **Belco B.V.**, kantoorhoudende aan Messingstraat 10, 8472 EE Wolvega, ingeschreven in het Handelsregister onder nummer 57 869 480 (“**Belco**” of “**Verwerker**”).

Klant en Belco worden afzonderlijk aangeduid als “**Partij**” en gezamenlijk als “**Partijen**”.

Deze Verwerkersovereenkomst maakt integraal deel uit van de overeenkomst waaronder Belco de Dienst aan Klant levert (de “**Hoofdovereenkomst**”). Zij geldt voor Klant vanaf het moment waarop Klant haar elektronisch accepteert. Bij een nieuw account vindt die acceptatie plaats voordat Klant Persoonsgegevens in de Dienst laat verwerken.

1. Definities

1.1. Begrippen met een hoofdletter die niet in deze Verwerkersovereenkomst zijn gedefinieerd, hebben de betekenis die daaraan in de AVG of de Hoofdovereenkomst is gegeven.

1.2. In deze Verwerkersovereenkomst wordt verstaan onder:

- **AVG:** Verordening (EU) 2016/679 (Algemene verordening gegevensbescherming) en de toepasselijke Nederlandse uitvoeringswetgeving;
- **Betrokkene:** de geïdentificeerde of identificeerbare natuurlijke persoon op wie Klantgegevens betrekking hebben;
- **Dienst:** de door Belco aangeboden SaaS-dienst voor klantcommunicatie en klantenservice, met de door Klant geactiveerde functies en integraties;
- **Datalek:** een inbreuk in verband met Persoonsgegevens als bedoeld in artikel 4, onderdeel 12, AVG;
- **Juridische Pagina:** de pagina op <https://www.belco.nl/terms-and-conditions>, waarop Belco haar actuele juridische documenten en subverwerkersregister beschikbaar stelt;
- **Klantgegevens:** Persoonsgegevens die Belco in het kader van de Dienst namens Klant verwerkt;
- **Subverwerker:** een derde die Belco inschakelt om Klantgegevens namens Klant te verwerken;
- **Toeziethouder:** de bevoegde onafhankelijke gegevensbeschermingsautoriteit;
- **Verwerking:** iedere bewerking van Persoonsgegevens als bedoeld in artikel 4, onderdeel 2, AVG.

1.3. Gegevens die Belco voor eigen, zelfstandig bepaalde doeleinden verwerkt, zoals gegevens voor facturatie, debiteurenbeheer, fraudepreventie, contractadministratie en het bewijs van acceptatie van juridische documenten, vallen niet onder de opdrachtverwerking in deze Verwerkersovereenkomst. Voor die Verwerkingen is Belco zelfstandig Verwerkingsverantwoordelijke en geldt de privacyverklaring van Belco.

2. Onderwerp, toepasselijkheid en rangorde

2.1. Deze Verwerkersovereenkomst regelt de Verwerking van Klantgegevens door Belco bij de uitvoering van de Dienst. De details van de Verwerking staan in Bijlage 1.

2.2. Klant bepaalt de doeleinden en wezenlijke middelen van de Verwerking van Klantgegevens. Belco verwerkt Klantgegevens uitsluitend voor Klant en binnen de grenzen van de gedocumenteerde instructies van Klant, tenzij Partijen voor een specifieke Verwerking feitelijk een andere rol hebben.

2.3. De feitelijke omstandigheden en de AVG bepalen de rol van iedere Partij. Een contractuele kwalificatie die niet met de feiten overeenkomt, wijzigt die wettelijke rol niet.

2.4. Bij strijdigheid geldt voor onderwerpen over de Verwerking van Klantgegevens de volgende rangorde:

1. dwingend toepasselijk gegevensbeschermingsrecht;

2. toepasselijke standaardcontractbepalingen voor internationale doorgifte;
3. deze Verwerkersovereenkomst, inclusief haar bijlagen;
4. de Hoofdovereenkomst;
5. overige documentatie.

2.5. Deze Verwerkersovereenkomst geeft Belco geen recht om Klantgegevens te verkopen of te gebruiken voor eigen reclame, profilering voor eigen doeleinden of training van generieke AI-modellen. Een dergelijke Verwerking vereist een afzonderlijk vastgelegde rol, grondslag en afspraak.

2.6. Informatie valt alleen buiten deze Verwerkersovereenkomst wanneer zij zodanig is geanonimiseerd dat herleiding tot een natuurlijke persoon redelijkerwijs niet meer mogelijk is. Pseudonimisering alleen is geen anonimisering.

3. Gedocumenteerde instructies

3.1. Belco verwerkt Klantgegevens uitsluitend:

- om de Dienst overeenkomstig de Hoofdovereenkomst te leveren, te beveiligen, te onderhouden en te ondersteunen;
- volgens de door Klant gebruikte instellingen, rollen, workflows, integraties en opdrachten in de Dienst;
- volgens aanvullende schriftelijke of elektronisch vastgelegde instructies die binnen de afgesproken functionaliteit en de wet passen; en
- zoals nader omschreven in Bijlage 1.

3.2. De Hoofdovereenkomst, deze Verwerkersovereenkomst, de configuratie van de Dienst en aantoonbare opdrachten via het account of supportkanaal vormen samen de gedocumenteerde instructies van Klant.

3.3. Als Belco op grond van Unierecht of Nederlands recht verplicht is Klantgegevens anders te verwerken, informeert Belco Klant vóór die Verwerking over de wettelijke verplichting, tenzij de wet dat om gewichtige redenen van algemeen belang verbiedt.

3.4. Indien Belco van mening is dat een instructie inbreuk maakt op de AVG of ander toepasselijk gegevensbeschermingsrecht, informeert Belco Klant daarover zonder onredelijke vertraging. Belco mag de uitvoering van de betreffende instructie opschorten totdat Klant haar heeft bevestigd of aangepast, voor zover opschorting nodig is om een mogelijke overtreding te voorkomen.

3.5. Een instructie die buiten de overeengekomen Dienst valt of onevenredige werkzaamheden vereist, wordt uitgevoerd na overleg over haalbaarheid, planning en redelijke kosten. Deze bepaling beperkt de wettelijke verplichtingen van Belco niet.

4. Verplichtingen van Klant

4.1. Klant is verantwoordelijk voor de rechtmatigheid van de Verwerking van Klantgegevens en zorgt ervoor dat zij:

- een geldige grondslag heeft voor de Verwerking en verstrekking aan Belco;
- Betrokkenen tijdig en correct informeert;
- alleen Persoonsgegevens laat verwerken die passend, relevant en noodzakelijk zijn;
- bewaartermijnen, toegangsrechten, integraties en overige instellingen passend configureert;
- instructies geeft die in overeenstemming zijn met de AVG;
- verzoeken van Betrokkenen en meldingen aan de Toezichthouder afhandelt; en
- gebruikersaccounts, rollen, inlogmiddelen en gekoppelde externe diensten zorgvuldig beheert.

4.2. Klant gebruikt de Dienst niet voor stelselmatige Verwerking van bijzondere categorieën Persoonsgegevens, strafrechtelijke Persoonsgegevens, nationale identificatienummers of andere gegevens met een uitzonderlijk hoog risico, tenzij dit noodzakelijk en rechtmatig is en Partijen vooraf schriftelijk passende aanvullende maatregelen hebben afgesproken. Incidentele opname van zulke gegevens in klantcommunicatie ontslaat Partijen niet van hun wettelijke verplichtingen.

4.3. Klant voorkomt dat wachtwoorden, geheime sleutels of volledige betaalkaartgegevens in vrije tekstvelden, berichten of bijlagen worden opgenomen, behalve voor zover een specifiek onderdeel van de Dienst daarvoor uitdrukkelijk is ingericht.

5. Geheimhouding en personeel

5.1. Belco waarborgt dat personen die onder haar gezag toegang hebben tot Klantgegevens:

- alleen toegang krijgen voor zover dat noodzakelijk is voor hun taak;
- Klantgegevens uitsluitend volgens de instructies van Klant verwerken;
- contractueel of wettelijk tot vertrouwelijkheid zijn verplicht; en
- passende instructie krijgen over gegevensbescherming en informatiebeveiliging.

5.2. De geheimhoudingsplicht blijft gelden na beëindiging van de werkzaamheden of deze Verwerkersovereenkomst.

5.3. Belco beheert toegangsrechten gedurende de gehele levenscyclus van een account of functie. Bevoorrechte toegang wordt beperkt en gecontroleerd overeenkomstig Bijlage 2.

6. Beveiliging

6.1. Belco treft en onderhoudt passende technische en organisatorische maatregelen zoals bedoeld in artikel 32 AVG. Bijlage 2 beschrijft de categorieën maatregelen die Belco voor de Dienst toepast.

6.2. Bij het bepalen van passende maatregelen houdt Belco rekening met de stand van de techniek, uitvoeringskosten, aard, omvang, context en doeleinden van de Verwerking en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor Betrokkenen.

6.3. Belco mag maatregelen aanpassen aan technische ontwikkelingen en gewijzigde risico's, mits het algemene beschermingsniveau niet wezenlijk wordt verlaagd.

6.4. Klant erkent dat beveiliging een gedeelde verantwoordelijkheid is. Klant is onder meer verantwoordelijk voor een passende rollenstructuur, het tijdig intrekken van accounts, veilige eindapparaten, het beschermen van inlogmiddelen, het instellen van beschikbare beveiligingsopties en de beveiliging van door Klant gekozen integraties.

6.5. Geen enkele beveiligingsmaatregel kan alle incidenten voorkomen. Dit doet niet af aan de verplichting van Belco om aantoonbaar passende maatregelen te treffen.

7. Datalekken

7.1. Belco informeert Klant zonder onredelijke vertraging nadat Belco kennis heeft genomen van een Datalek dat betrekking heeft op Klantgegevens.

7.2. De melding bevat, voor zover de informatie op dat moment beschikbaar is:

- de aard van het Datalek;
- de categorieën en bij benadering het aantal betrokken Betrokkenen;
- de categorieën en bij benadering het aantal betrokken persoonsgegevensrecords;
- de waarschijnlijke gevolgen;
- de getroffen of voorgestelde maatregelen om het Datalek te beëindigen en de gevolgen te beperken; en
- een contactpunt voor nadere informatie.

7.3. Indien niet alle informatie tegelijk beschikbaar is, verstrekt Belco de informatie gefaseerd zonder verdere onredelijke vertraging.

7.4. Belco neemt redelijke maatregelen om het Datalek te onderzoeken, te beperken en herhaling te helpen voorkomen. Belco houdt een incidentregister bij voor zover de AVG dat vereist.

7.5. Klant beslist of melding aan een Toezichthouder of communicatie aan Betrokkenen nodig is. Belco verleent, rekening houdend met de aard van de Verwerking en de beschikbare informatie, redelijke bijstand bij die beoordeling en melding. Belco doet geen melding namens Klant zonder instructie, tenzij de wet dat vereist.

7.6. Een melding of samenwerking vormt op zichzelf geen erkenning van aansprakelijkheid of tekortkoming.

8. Rechten van Betrokkenen

8.1. Rekening houdend met de aard van de Verwerking helpt Belco Klant met passende technische en organisatorische maatregelen om verzoeken van Betrokkenen uit te voeren, waaronder inzage, rectificatie, wissing, beperking, overdraagbaarheid en bezwaar, voor zover deze rechten van toepassing zijn.

8.2. Wanneer een Betrokkene zich rechtstreeks tot Belco richt over Klantgegevens, stuurt Belco het verzoek zonder onredelijke vertraging door aan Klant en reageert Belco niet inhoudelijk, behalve op instructie van Klant of wanneer de wet dit vereist.

8.3. Voor zover Klant een verzoek zelfstandig via de standaardfunctionaliteit kan uitvoeren, gebruikt Klant die functionaliteit eerst. Aanvullende bijstand die buiten de standaardfunctionaliteit valt, kan na voorafgaand overleg tegen redelijke kosten worden geleverd, zonder afbreuk te doen aan dwingende wettelijke verplichtingen.

9. Bijstand bij naleving

9.1. Rekening houdend met de aard van de Verwerking en de informatie waarover Belco beschikt, verleent Belco redelijke bijstand bij de naleving door Klant van de artikelen 32 tot en met 36 AVG, waaronder:

- beveiliging van de Verwerking;
- beoordeling en melding van Datalekken;
- een gegevensbeschermingseffectbeoordeling; en
- een eventuele voorafgaande raadpleging van een Toezichthouder.

9.2. Belco verstrekt op redelijk verzoek informatie over de Dienst die Klant nodig heeft voor haar risicoanalyse of gegevensbeschermingseffectbeoordeling. Klant blijft verantwoordelijk voor het uitvoeren en documenteren daarvan.

9.3. Indien de gevraagde bijstand wezenlijk verder gaat dan de standaarddienstverlening, mogen Partijen redelijke kosten en een planning afspreken. Dit maakt wettelijk noodzakelijke en tijdkritische bijstand niet feitelijk onmogelijk.

10. Subverwerkers

10.1. Klant geeft Belco algemene schriftelijke toestemming om Subverwerkers in te schakelen voor de uitvoering van de Dienst.

10.2. Belco houdt op de Juridische Pagina een actueel subverwerkersregister bij. Dat register maakt integraal deel uit van deze Verwerkersovereenkomst en vermeldt per Subverwerker ten minste de gebruikte dienst, het doel van de Verwerking en, indien relevant, informatie over internationale doorgifte.

10.3. De bij publicatie van versie 2.0 daadwerkelijk gebruikte diensten staan in Bijlage 3. Het actuele online register is leidend voor latere toevoegingen en vervangingen, met inachtneming van de kennisgevings- en bezwaarprocedure in dit artikel.

10.4. Belco legt iedere Subverwerker schriftelijk materieel dezelfde gegevensbeschermingsverplichtingen op als de verplichtingen die voor de betreffende Verwerking uit deze Verwerkersovereenkomst volgen, waaronder passende beveiliging, vertrouwelijkheid, bijstand, verwijdering en regels voor internationale doorgifte.

10.5. Belco blijft tegenover Klant volledig verantwoordelijk voor de nakoming van de verplichtingen van haar Subverwerkers, voor zover artikel 28, vierde lid, AVG dat bepaalt.

10.6. Belco informeert Klant rechtstreeks, via het bij het account geregistreerde e-mailadres en/of een duidelijke melding in de Dienst, ten minste 30 dagen vóór het toevoegen of vervangen van een Subverwerker. Indien een versnelde wijziging noodzakelijk is om een ernstig beveiligingsrisico te beperken, de continuïteit te waarborgen of aan de wet te voldoen, informeert Belco Klant zo spoedig mogelijk en licht zij de reden voor de kortere termijn toe.

10.7. Klant kan binnen 14 dagen na de kennisgeving gemotiveerd bezwaar maken op redelijke gronden die rechtstreeks verband houden met de bescherming van Klantgegevens. Partijen overleggen vervolgens in goed vertrouwen over een redelijke oplossing. Als geen redelijke oplossing beschikbaar is, mag Klant het aantoonbaar geraakte onderdeel van de Dienst beëindigen of, wanneer dat onderdeel wezenlijk is, de Hoofdovereenkomst beëindigen volgens de daarin opgenomen procedure.

10.8. Een externe dienst die Klant zelf kiest, activeert of koppelt en die rechtstreeks onder instructie of verantwoordelijkheid van Klant handelt, is niet automatisch een Subverwerker van Belco. De feitelijke rolverdeling blijft doorslaggevend.

10.9. Software die Belco op eigen infrastructuur uitvoert zonder dat de softwareleverancier toegang krijgt tot Klantgegevens, is op zichzelf geen Subverwerker. De aanbieder van de onderliggende infrastructuur kan dat wel zijn en wordt in dat geval in het actuele register opgenomen.

11. Internationale doorgiften

- 11.1. Belco geeft Klantgegevens alleen door aan een land buiten de Europese Economische Ruimte of een internationale organisatie op basis van een geldige doorgiftegrond uit hoofdstuk V AVG.
- 11.2. Een geldige doorgiftegrond kan bestaan uit een toepasselijk adequaatheidsbesluit van de Europese Commissie, toepasselijke standaardcontractbepalingen van de Europese Commissie of een andere wettelijk toegestane waarborg.
- 11.3. Indien standaardcontractbepalingen worden gebruikt, past Belco de module toe die aansluit op de feitelijke rollen. Voor een doorgifte van Belco als Verwerker aan een Subverwerker is dit in beginsel de module voor verwerker naar verwerker.
- 11.4. Belco beoordeelt waar vereist de wetgeving en praktijk in het derde land en treft aanvullende technische, contractuele of organisatorische maatregelen wanneer dat nodig is om een in wezen gelijkwaardig beschermingsniveau te waarborgen.
- 11.5. Een beroep op het EU-US Data Privacy Framework vindt alleen plaats wanneer de betreffende Amerikaanse ontvanger voor de relevante gegevenscategorieën geldig is gecertificeerd. Valt die grond weg, dan zorgt Belco vóór verdere doorgifte voor een andere geldige waarborg of staakt zij de doorgifte.
- 11.6. Het actuele subverwerkersregister en Bijlage 4 beschrijven hoe Belco internationale doorgiften beheert. Belco doet geen algemene toezegging dat gegevens uitsluitend binnen de EER blijven, tenzij zij dit voor een specifieke dienst uitdrukkelijk schriftelijk bevestigt.
- 11.7. Wanneer Klant zelf een integratie activeert die tot een doorgifte buiten de EER leidt, geldt die activering als gedocumenteerde instructie voor de technisch noodzakelijke doorgifte. Dit ontslaat geen van beide Partijen van hoofdstuk V AVG. Sluit Klant rechtstreeks een overeenkomst met de externe ontvanger, dan is Klant verantwoordelijk voor de doorgiftewaarborg die bij haar rol hoort. Schakelt Belco de ontvanger als Subverwerker in, dan is Belco verantwoordelijk voor de waarborg die bij haar rol hoort.

12. Verzoeken van overheidsinstanties

- 12.1. Belco verstrekt Klantgegevens aan een overheidsinstantie uitsluitend wanneer zij daartoe wettelijk verplicht is.
- 12.2. Voor zover wettelijk toegestaan informeert Belco Klant vóór verstrekking over het verzoek. Indien voorafgaande informatie verboden is, informeert Belco Klant zodra dat rechtmatig mogelijk is.
- 12.3. Belco beoordeelt of het verzoek geldig, bindend, specifiek en proportioneel is en beperkt de verstrekking of maakt bezwaar waar daarvoor redelijke juridische gronden bestaan. Belco verstrekt niet meer Klantgegevens dan wettelijk vereist.

13. Aantoonbaarheid en audits

- 13.1. Belco stelt alle informatie ter beschikking die redelijkerwijs nodig is om aan te tonen dat zij de verplichtingen uit artikel 28 AVG en deze Verwerkersovereenkomst nakomt.
- 13.2. Belco mag in eerste instantie gebruikmaken van beschikbare onafhankelijke assurance-rapporten, certificeringen, samenvattingen van beveiligingstesten, vragenlijsten en andere passende bewijsstukken. Het ontbreken van een certificering betekent niet automatisch dat niet aan artikel 32 AVG wordt voldaan.
- 13.3. Indien de beschikbare informatie redelijkerwijs onvoldoende is, mag Klant zelf of via een onafhankelijke, deskundige auditor een audit uitvoeren. Daarbij geldt:
- Klant kondigt de audit in beginsel ten minste 30 dagen vooraf schriftelijk aan;
 - de audit vindt in beginsel tijdens normale kantooruren en eenmaal per twaalf maanden plaats;
 - de auditor is geen directe concurrent van Belco en is aan passende geheimhouding gebonden;
 - de audit beperkt zich tot systemen, processen en informatie die relevant zijn voor Klantgegevens;
 - de audit verstoort de Dienst niet onnodig en beschermt gegevens en vertrouwelijke informatie van andere klanten; en
 - Partijen gebruiken waar mogelijk veilige bewijsvoering op afstand voordat toegang op locatie wordt gevraagd.
- 13.4. De beperkingen in artikel 13.3 gelden niet voor zover een Toezichthouder anders verlangt of wanneer een Datalek, concrete aanwijzing van wezenlijke niet-naleving of een wettelijk urgente situatie een snellere of aanvullende audit redelijkerwijs noodzakelijk maakt.

13.5. Klant draagt de redelijke eigen en externe kosten van een audit, tenzij daaruit een wezenlijke tekortkoming van Belco blijkt. In dat geval draagt Belco haar eigen redelijke kosten en de redelijke kosten van de noodzakelijke hercontrole. Financiële afspraken mogen het wettelijke controlerecht niet feitelijk onmogelijk maken.

13.6. Belco werkt mee aan onderzoek van de bevoegde Toezichthouder voor zover de wet dat vereist.

14. Teruggave, export en verwijdering

14.1. Tijdens de looptijd biedt Belco Klant binnen de beschikbare functionaliteit mogelijkheden om Klantgegevens te raadplegen, te exporteren en te verwijderen. De ondersteunde formaten en beperkingen worden in de Dienst of productdocumentatie beschreven.

14.2. Na beëindiging van de Verwerkingsdiensten verwijdert Belco, naar keuze van Klant, alle Klantgegevens of geeft zij deze aan Klant terug, en verwijdert zij bestaande kopieën, tenzij Unierecht of Nederlands recht bewaring verplicht.

14.3. Klant deelt haar keuze uiterlijk bij beëindiging mee. Als Klant geen keuze maakt, verwijdert Belco de Klantgegevens volgens haar vastgelegde verwijderproces. Belco informeert Klant over de beschikbare exportmogelijkheid voordat verwijdering definitief wordt.

14.4. Belco voert teruggave en verwijdering zonder onredelijke vertraging uit. Gegevens in back-ups worden volgens de reguliere, beveiligde back-upcyclus overschreven of verwijderd en blijven tot dat moment afgeschermd van ander gebruik, behoudens noodzakelijk herstel of een wettelijke verplichting.

14.5. Gegevens die wettelijk moeten worden bewaard, worden afgeschermd, alleen voor dat wettelijke doel gebruikt en verwijderd zodra de bewaarplicht eindigt.

14.6. Op redelijk verzoek bevestigt Belco schriftelijk dat de verwijdering overeenkomstig dit artikel is uitgevoerd.

15. Duur en einde

15.1. Deze Verwerkersovereenkomst vangt aan bij elektronische acceptatie en blijft van kracht zolang Belco namens Klant Klantgegevens verwerkt, ook tijdens een gratis proefperiode.

15.2. Beëindiging van de Hoofdovereenkomst beëindigt deze Verwerkersovereenkomst niet zolang Belco nog Klantgegevens verwerkt of bewaart.

15.3. Bepalingen die naar hun aard na beëindiging behoren voort te duren, waaronder geheimhouding, audit over de relevante voorafgaande periode, verwijdering, internationale doorgifte en aansprakelijkheid, blijven gelden zolang dat nodig is.

16. Elektronische acceptatie en bewijs

16.1. Deze Verwerkersovereenkomst kan overeenkomstig artikel 28, negende lid, AVG elektronisch worden gesloten. Acceptatie kan plaatsvinden via een niet vooraf aangevinkte checkbox of via een duidelijke acceptatietekst met verwijzing naar de documenten direct bij de knop waarmee een trial wordt gestart, een betaald account wordt geactiveerd of bijgewerkte juridische documenten worden bevestigd.

16.2. Binnen een bestaande organisatie kan de acceptatie worden uitgevoerd door een gebruiker met de accountrol **owner** of **admin**. Klant is verantwoordelijk voor de correcte toekenning en tijdige intrekking van die rollen. In de upgradeflow is geen afzonderlijke bevoegdheidsverklaring vereist. Belco bewaart het beschikbare bewijs van de geauthenticeerde handeling en, bij een betaald Abonnement, de activering of betaling.

16.3. Belco registreert ten behoeve van bewijs en compliance de gegevens die in de gebruikte acceptatiestroom beschikbaar en noodzakelijk zijn. Dit kan onder meer omvatten:

- organisatie-ID en organisatienaam;
- gebruiker-ID, naam en e-mailadres zoals geregistreerd op het moment van acceptatie;
- datum en tijd in UTC, server-side vastgelegd;
- brongebeurtenis, zoals `trial_signup`, `paid_upgrade` of `legal_update`;
- taal, versienummer en document-ID van de geaccepteerde Algemene Voorwaarden en Verwerkersovereenkomst;
- een cryptografische hash, document-ID, publicatiearchief of een andere betrouwbare identificatie van de toepasselijke documenten;
- de getoonde acceptatietekst en knoptekst, voor zover deze wordt vastgelegd; en

- IP-adres en, voor zover proportioneel, user-agent of sessie-ID.

16.4. Belco beschermt bewaard acceptatiebewijs tegen ongeautoriseerde wijziging, beperkt de toegang en bewaart het niet langer dan nodig voor contractbewijs, wettelijke verplichtingen en de verjaring of afwikkeling van rechtsvorderingen. Belco verwerkt deze bewijsgegevens als zelfstandig Verwerkingsverantwoordelijke overeenkomstig toepasselijk privacyrecht.

16.5. Klant kan op verzoek een afschrift van de geaccepteerde versie en de voor haar organisatie geregistreeerde acceptatiegegevens ontvangen.

17. Wijzigingen en kennisgeving

17.1. Belco mag deze Verwerkersovereenkomst wijzigen wanneer dat nodig is door gewijzigde wetgeving, aanwijzingen van toezichthouders, gewijzigde Verwerkingen of een materiële wijziging van de Dienst.

17.2. Een inhoudelijke wijziging wordt ten minste 30 dagen vóór de beoogde ingangsdatum rechtstreeks aan Klant gemeld via het geregistreeerde e-mailadres en/of een duidelijke melding in de Dienst. De melding bevat de nieuwe versie, ingangsdatum en een begrijpelijke samenvatting van de wijzigingen.

17.3. Een inhoudelijk gewijzigde Verwerkersovereenkomst treedt voor Klant pas in werking nadat een owner of admin deze elektronisch heeft geaccepteerd, behalve voor zover dwingend recht een eerdere toepassing vereist. Alleen publicatie op een website of voortgezet gebruik geldt niet als goedkeuring van een inhoudelijk gewijzigde Verwerkersovereenkomst.

17.4. Indien Klant de gewijzigde versie niet vóór de aangekondigde datum accepteert, blijft de bestaande versie gelden zolang Belco rechtmatig onder die versie kan blijven verwerken. Indien de wijziging noodzakelijk is om de Dienst rechtmatig of veilig te blijven leveren, kan Belco na een aanvullende redelijke termijn de toegang tot Verwerkingen opschorten of de Hoofdovereenkomst volgens haar bepalingen beëindigen. Belco geeft Klant vooraf een redelijke mogelijkheid om Klantgegevens te exporteren.

17.5. Artikel 17.3 geldt niet voor:

- een wijziging in Subverwerkers volgens artikel 10, waarvoor de daar beschreven algemene toestemming en bezwaarprocedure geldt;
- een redactionele correctie zonder inhoudelijk effect; of
- een wijziging in Bijlage 2 die het algemene beschermingsniveau niet wezenlijk verlaagt.

17.6. Iedere gepubliceerde versie krijgt een uniek versienummer, ingangsdatum en onveranderbare kopie. Belco archiveert voorgaande versies voor bewijsdoeleinden.

17.7. Versie 2.0 geldt vanaf de werkelijke acceptatiedatum en wordt niet teruggedateerd. Belco bewaart eerdere versies en bestaande acceptatiegegevens zodat kan worden vastgesteld welke versie in welke periode gold.

18. Aansprakelijkheid

18.1. De aansprakelijkheidsregeling uit de Hoofdovereenkomst is van toepassing, voor zover dat wettelijk is toegestaan en deze niet in strijd is met de AVG.

18.2. Niets in deze Verwerkersovereenkomst beperkt rechten van Betrokkenen of aansprakelijkheid die op grond van artikel 82 AVG of ander dwingend recht niet contractueel kan worden uitgesloten of beperkt.

18.3. Iedere Partij is verantwoordelijk voor de schade en kosten die voortvloeien uit haar eigen handelen of nalaten, overeenkomstig de feitelijke rolverdeling en toepasselijke wetgeving.

19. Contact en kennisgevingen

19.1. Privacy- en beveiligingsmeldingen aan Belco worden gestuurd aan hello@belco.io.

19.2. Belco stuurt kennisgevingen aan het primaire e-mailadres van de organisatie en/of aan owners en admins in de Dienst. Klant houdt deze gegevens actueel.

19.3. Een Datalek of spoedeisend beveiligingsincident wordt via een als zodanig herkenbaar kanaal gemeld en niet uitsluitend via een openbare webpagina.

20. Taal, toepasselijk recht en slotbepalingen

20.1. Belco stelt deze Verwerkersovereenkomst in het Nederlands en Engels beschikbaar met hetzelfde versienummer en dezelfde inhoud. De Nederlandstalige versie is het brondocument. Bij verschil in uitleg prevaleert de Nederlandstalige versie, tenzij Partijen in een schriftelijke overeenkomst uitdrukkelijk hebben vastgelegd dat de Engelse versie prevaleert. Dwingend recht blijft altijd voorgaan.

20.2. Op deze Verwerkersovereenkomst is Nederlands recht van toepassing. De geschillenregeling uit de Hoofdovereenkomst geldt ook voor deze Verwerkersovereenkomst, voor zover dwingend recht of de bevoegdheid van een Toezichthouder niet anders bepaalt.

20.3. Indien een bepaling nietig, vernietigbaar of onafdwingbaar is, blijven de overige bepalingen van kracht. Partijen vervangen de betreffende bepaling door een geldige bepaling die doel en strekking zo dicht mogelijk benadert zonder de AVG te beperken.

20.4. Afstand van een recht is alleen geldig wanneer deze uitdrukkelijk en schriftelijk is gedaan en geldt uitsluitend voor het betreffende geval.

Bijlage 1 — Details van de Verwerking

1. Onderwerp

Belco verwerkt Klantgegevens om Klant de Belco-dienst voor klantcommunicatie en klantenservice te leveren. Afhankelijk van de door Klant gekozen configuratie kan dit bestaan uit:

- ontvangen, verzenden, routeren, tonen, zoeken, labelen en bewaren van klantcommunicatie;
- samenwerken aan en afhandelen van gesprekken en tickets;
- beheren van contacten, gebruikers, teams, rollen, tags, notities en workflows;
- koppelen van communicatiekanalen en externe systemen;
- tonen van context uit gekoppelde webwinkels of andere bronnen;
- technische ondersteuning, probleemonderzoek en herstel op verzoek van Klant; en
- beveiliging, misbruikdetectie, logging, back-up en continuïteit van de Dienst.

2. Duur

De Verwerking duurt vanaf het eerste moment waarop Klant Klantgegevens in de trial of betaalde Dienst laat verwerken totdat de gegevens overeenkomstig artikel 14 zijn teruggegeven of verwijderd.

3. Aard en frequentie

De Verwerking kan bestaan uit verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken, opvragen, raadplegen, gebruiken, doorzenden, beschikbaar stellen, combineren, beperken, exporteren, archiveren en verwijderen. Zij vindt doorlopend of op verzoek plaats zolang Klant de relevante functies gebruikt.

4. Doeleinden

Belco verwerkt Klantgegevens uitsluitend voor:

1. levering van de geconfigureerde Dienst;
2. uitvoering van opdrachten en workflows van Klant;
3. beschikbaarheid, integriteit, vertrouwelijkheid en herstel van de Dienst;
4. technische support en foutanalyse;
5. voorkoming en onderzoek van misbruik en beveiligingsincidenten; en
6. nakoming van een rechtstreeks op Belco rustende wettelijke plicht overeenkomstig artikel 3.3.

Gebruik voor eigen marketing of training van generieke AI-modellen is geen onderdeel van deze doeleinden.

5. Categorieën Betrokkenen

Afhankelijk van het gebruik door Klant kunnen Klantgegevens betrekking hebben op:

- klanten, voormalige klanten, prospects en leads van Klant;
- bezoekers en gebruikers van websites, webwinkels, apps en communicatiekanalen van Klant;
- kopers, ontvangers, retouraanvragers en contactpersonen bij bestellingen;
- werknemers, uitzendkrachten, opdrachtnemers, agenten en accountgebruikers van Klant;
- leveranciers, zakelijke partners en andere contactpersonen van Klant; en
- personen die deelnemen aan of worden genoemd in e-mails, chats, telefoongesprekken, sociale berichten of bijlagen.

6. Categorieën Persoonsgegevens

Afhankelijk van wat Klant invoert of koppelt, kunnen de volgende categorieën worden verwerkt:

- identificatie- en contactgegevens, zoals naam, bedrijfsnaam, adres, e-mailadres, telefoonnummer, gebruikersnaam en profielfoto;
- account- en autorisatiegegevens, zoals organisatie, rol, teams, kanaalidentificatoren en externe account-ID's;
- inhoud van communicatie, zoals e-mails, chatberichten, sociale berichten, WhatsApp-berichten, interne notities, eventuele transcripties en bijlagen;
- gegevens over bestellingen en klantrelaties, zoals ordernummer, producten, levering, retouren, status, bedragen en klantgeschiedenis, voor zover via een integratie beschikbaar;
- telefoniegegevens, zoals nummer, gesprekstijdstip, duur en, uitsluitend indien geactiveerd en rechtmatig, een gespreksopname of transcriptie;
- technische en gebruiksgegevens, zoals IP-adres, tijdstippen, browser- of apparaatkenmerken, loggegevens, foutmeldingen en auditgebeurtenissen;
- labels, prioriteiten, routeringsinformatie, voorkeuren en andere door Klant bepaalde metadata;
- authenticatietokens of integratiegegevens die nodig zijn om een gekoppelde dienst te laten functioneren; en
- bijzondere of strafrechtelijke Persoonsgegevens die Betrokkenen of Klant incidenteel in vrije communicatie opnemen, hoewel de Dienst niet is bedoeld voor structurele Verwerking daarvan zonder aanvullende afspraken.

Volledige betaalkaartgegevens behoren niet tot de beoogde Klantgegevens.

7. Bewaring

Klantgegevens worden verwerkt zolang dit nodig is om de Dienst te leveren, volgens de door Klant gekozen instellingen en toepasselijke wettelijke verplichtingen. Operationele logs, beveiligingslogs, tijdelijke supportbestanden en back-ups worden alleen bewaard zolang zij redelijkerwijs nodig zijn voor beveiliging, ondersteuning, herstel en continuïteit. Na beëindiging gelden artikel 14 en de reguliere, beveiligde verwijdercycli van Belco en haar Subverwerkers.

8. Rechten en verplichtingen van Klant

Klant heeft de rechten en verplichtingen zoals opgenomen in de AVG, de Hoofdovereenkomst en deze Verwerkersovereenkomst. Klant mag onder meer instructies geven, instellingen beheren, informatie opvragen, een audit uitvoeren, export of verwijdering verzoeken en bezwaar maken tegen een nieuwe Subverwerker volgens de overeengekomen procedures.

9. Aanvullende instructies

Aanvullende instructies worden vastgelegd via de accountinstellingen, een supportticket, e-mail of een door Partijen ondertekend document. Mondelinge instructies worden door Belco schriftelijk bevestigd voordat zij worden uitgevoerd, tenzij onmiddellijk handelen nodig is om een incident te beperken.

Bijlage 2 — Technische en organisatorische maatregelen

Belco onderhoudt een op risico gebaseerd informatiebeveiligingsprogramma dat passend is bij de Dienst en de aard van de Klantgegevens. De maatregelen worden periodiek en na relevante wijzigingen of incidenten beoordeeld.

1. Governance en risicobeheer

Belco wijst verantwoordelijkheden voor informatiebeveiliging en privacy toe en onderhoudt beleid en werkafspraken voor toegangsbeheer, wijzigingen, incidenten, back-up, verwijdering en leveranciers. Relevante risico's, incidenten en kwetsbaarheden worden passend geregistreerd, beoordeeld en opgevolgd.

2. Identiteits- en toegangsbeheer

Belco gebruikt persoonlijke accounts, rolgebaseerde toegang en het beginsel van minimale rechten. Toegangsrechten worden beheerd bij indiensttreding, functiewijziging en uitdiensttreding en worden naar risico periodiek beoordeeld. Bevoorrechte toegang wordt extra beperkt en, waar passend en technisch beschikbaar, met meervoudige authenticatie beschermd.

3. Encryptie en geheimen

Belco beschermt Klantgegevens tijdens transport met actuele, algemeen aanvaarde beveiligde protocollen. Opgeslagen gegevens, back-ups, sleutels, tokens en andere geheimen worden beschermd met maatregelen die passen bij het risico en de gebruikte infrastructuur. Wachtwoorden worden niet bewust in leesbare vorm opgeslagen.

4. Scheiding en minimalisatie

Belco past logische scheiding tussen organisaties en autorisatiecontroles op organisatiegegevens toe. Productie, test en ontwikkeling worden met passende technische of organisatorische controles van elkaar gescheiden. Productiegegevens worden niet routinematig voor ontwikkeling of tests gebruikt en worden, wanneer gebruik noodzakelijk is, beperkt en waar mogelijk geanonimiseerd of gepseudonimiseerd.

5. Veilige ontwikkeling en wijzigingen

Wijzigingen aan de Dienst worden via een beheerst proces ontwikkeld, beoordeeld, getest en uitgerold in verhouding tot het risico. Toegang tot broncode en uitrolmogelijkheden is beperkt. Afhankelijkheden en relevante kwetsbaarheidsmeldingen worden beoordeeld en beveiligingsrelevante fouten worden naar risico opgevolgd.

6. Logging, monitoring en detectie

Belco logt en bewaakt operationele en beveiligingsrelevante gebeurtenissen voor zover passend voor beschikbaarheid, foutanalyse, misbruikdetectie en incidentonderzoek. Toegang tot logs wordt beperkt en de inhoud en bewaartermijn worden afgestemd op noodzaak en risico.

7. Kwetsbaarheids- en patchbeheer

Belco beoordeelt en verwerkt beveiligingsupdates en bekende kwetsbaarheden naar ernst, blootstelling en risico. Publiek bereikbare onderdelen en kritieke afhankelijkheden worden passend gecontroleerd. Technische beveiligingstests worden met een omvang en frequentie uitgevoerd die bij het risico passen.

8. Beschikbaarheid, back-up en herstel

Belco gebruikt back-ups of gelijkwaardige herstelvoorzieningen voor gegevens en configuraties die voor herstel nodig zijn. Toegang tot herstelvoorzieningen wordt beperkt. Herstelprocedures worden periodiek getest of anderszins gevalideerd, rekening houdend met het belang van de betreffende systemen.

9. Incidentrespons

Belco onderhoudt een procedure voor detectie, classificatie, beheersing, onderzoek, herstel en evaluatie van beveiligingsincidenten. Relevante incidenten worden intern geëscaleerd, bewijs wordt passend beschermd en corrigerende maatregelen worden opgevolgd. Meldingen aan Klant vinden plaats overeenkomstig artikel 7.

10. Personeel

Personen met toegang tot Klantgegevens zijn contractueel of wettelijk tot geheimhouding verplicht en ontvangen beveiligings- en privacy-instructies die passen bij hun functie. Toegang tot systemen en bedrijfsmiddelen wordt bij functiewijziging en vertrek aangepast of ingetrokken.

11. Leveranciersbeheer

Belco beoordeelt Subverwerkers op relevante beveiligings-, privacy- en continuïteitsrisico's en maakt passende schriftelijke afspraken. Kritieke leveranciers worden naar risico opnieuw beoordeeld. Bij beëindiging wordt toegang ingetrokken en worden gegevens overeenkomstig de afspraken verwijderd of teruggegeven.

12. Fysieke beveiliging

Voor uitbestede hosting steunt Belco mede op de fysieke beveiligingsmaatregelen van haar infrastructuurleveranciers. Kantoor- en werkplekken en eventuele lokale opslag worden beschermd met maatregelen die passen bij de toegankelijke systemen en informatie.

13. Verwijdering en media

Belco gebruikt vastgelegde processen voor verwijdering of onomkeerbare overschrijving. Gegevens die uitsluitend nog in beveiligde back-ups aanwezig zijn, blijven beperkt toegankelijk totdat zij via de reguliere cyclus worden overschreven of verwijderd. Tijdelijke supportbestanden en exports worden verwijderd wanneer zij niet meer nodig zijn.

14. Continu verbeteren

Belco mag maatregelen vervangen door technisch of organisatorisch gelijkwaardige of betere maatregelen. Bevindingen uit incidenten, tests, audits, leveranciersbeoordelingen en gewijzigde risico's worden gebruikt om het beveiligingsprogramma te verbeteren.

Bijlage 3 — Actueel subverwerkersregister

Belco houdt het actuele subverwerkersregister bij op de Juridische Pagina. Dat online register is leidend en wordt gewijzigd volgens artikel 10. Niet iedere hieronder genoemde dienst wordt voor iedere Klant of functie gebruikt; een dienst is alleen Subverwerker voor zover zij daadwerkelijk Klantgegevens namens Belco verwerkt.

Op de publicatiedatum van versie 2.0 kunnen de volgende diensten, afhankelijk van de geactiveerde functies en technische route, bij de Verwerking van Klantgegevens worden gebruikt:

Dienst	Functie	Internationale doorgifte
Scalingo	Productiehosting, applicaties en databases	Primaire hosting in de EER
Amazon Web Services	Cloudinfrastructuur en opslagcomponenten, voor zover gebruikt	EER en/of derde landen; artikel 11 is van toepassing
DigitalOcean	AMQP-productie, workflow- en infrastructuurcomponenten, voor zover gebruikt	EER en/of derde landen; artikel 11 is van toepassing
Cloudflare	DNS, CDN, beveiliging en doorgifte van internetverkeer	Wereldwijd netwerk; artikel 11 is van toepassing waar nodig
Mailgun / Sinch	Transactionele e-mail en aflevermetadata	EER en/of derde landen; artikel 11 is van toepassing
Twilio	Communicatie- en telefoniediensten	EER en/of derde landen; artikel 11 is van toepassing
360dialog	WhatsApp Business-platform en berichtenverkeer	Afhankelijk van de gekozen WhatsApp-route; artikel 11 is van toepassing waar nodig
Speakup	Telefonie, nummer- en verkeersgegevens	Hoofdzakelijk EER; artikel 11 is van toepassing waar nodig
Axeos	Telefonieplatform en licentiecomponenten, voor zover gegevens worden verwerkt	Afhankelijk van de geactiveerde telefonieroute
WotNot	Chatbot- en AI-functionaliteit, voor zover door Klant geactiveerd	EER en/of derde landen; artikel 11 is van toepassing
Pushwoosh	Pushnotificaties en apparaatidentificatoren, voor zover gebruikt	EER en/of derde landen; artikel 11 is van toepassing
Monti APM	Applicatieprestatie monitoring, voor zover logs Klantgegevens bevatten	EER en/of derde landen; artikel 11 is van toepassing
Bunny.net	CDN en cloudopslag, voor zover gebruikt	Wereldwijd netwerk; artikel 11 is van toepassing waar nodig
ip-api / Artia International	IP-geolocatie, voor zover geactiveerd	EER en/of derde landen; artikel 11 is van toepassing waar nodig

Een andere leverancier wordt alleen als Subverwerker aangemerkt indien en voor zover deze daadwerkelijk Klantgegevens namens Belco verwerkt. Belco voegt zo'n leverancier vóór of bij aanvang van die Verwerking aan het actuele register toe en past de kennisgevings- en bezwaarprocedure uit artikel 10 toe.

Bijlage 4 — Internationale doorgiften

1. Uitgangspunt

Belco verwerkt Klantgegevens binnen of buiten de EER uitsluitend overeenkomstig artikel 11. Het actuele subverwerkersregister vermeldt bij een relevante Subverwerker of internationale doorgifte kan plaatsvinden en welke soort waarborg daarvoor wordt gebruikt.

2. Beoordeling en waarborgen

Voor een relevante doorgifte legt Belco naar toepasselijkheid vast:

- de betrokken partijen en hun rollen;
- de categorieën gegevens en Betrokkenen;
- het doel en de frequentie van de doorgifte;
- de landen van opslag of toegang;
- de toepasselijke doorgiftegrond;
- noodzakelijke aanvullende technische, contractuele of organisatorische maatregelen; en
- de uitkomst en herbeoordeling van een transfer impact assessment wanneer dat vereist is.

3. Standaardcontractbepalingen

Wanneer Belco standaardcontractbepalingen gebruikt, worden de toepasselijke bepalingen van de Europese Commissie door verwijzing onderdeel van de afspraken met de betreffende ontvanger. Bij strijdigheid over de internationale doorgifte gaan die standaardcontractbepalingen voor.

4. Wijziging of verval van een waarborg

Belco bewaakt voor zover redelijk de geldigheid van gebruikte doorgiftewaarborgen. Wanneer een adequaatheidsbesluit, certificering, standaardcontractbepaling of andere waarborg niet langer geldig of toereikend is, staakt Belco de betrokken doorgifte of implementeert zij zonder onredelijke vertraging een geldige vervangende waarborg. Belco informeert Klant wanneer de wijziging materieel is.

English text

The Dutch text prevails in the event of a conflict or difference in interpretation.

Parties

This data processing agreement (the “**DPA**”) is entered into between:

1. the legal entity or natural person acting in the course of a profession or business for which a Belco organisation account has been opened or which purchases a subscription to the Service, as registered in Belco by organisation name and billing details (the “**Customer**” or “**Controller**”); and
2. **Belco B.V.**, having its office at Messingstraat 10, 8472 EE Wolvega, the Netherlands, registered with the Dutch Chamber of Commerce under number 57 869 480 (“**Belco**” or “**Processor**”).

Customer and Belco are each referred to as a “**Party**” and together as the “**Parties**”.

This DPA forms an integral part of the agreement under which Belco provides the Service to Customer (the “**Main Agreement**”). It applies to Customer from the moment Customer accepts it electronically. For a new account, that acceptance takes place before Customer causes Personal Data to be processed in the Service.

1. Definitions

1.1. Capitalised terms not defined in this DPA have the meaning given to them in the GDPR or the Main Agreement.

1.2. In this DPA:

- **Customer Data:** Personal Data that Belco processes on behalf of Customer in connection with the Service;
- **Data Subject:** the identified or identifiable natural person to whom Customer Data relates;
- **GDPR:** Regulation (EU) 2016/679 (General Data Protection Regulation) and applicable Dutch implementing legislation;
- **Legal Page:** the page at <https://www.belco.nl/terms-and-conditions>, on which Belco makes its current legal documents and subprocessor register available;
- **Personal Data Breach:** a breach of security as referred to in Article 4(12) GDPR;
- **Processing:** any operation performed on Personal Data as referred to in Article 4(2) GDPR;
- **Service:** the SaaS service offered by Belco for customer communication and customer service, including the features and integrations activated by Customer;
- **Subprocessor:** a third party engaged by Belco to process Customer Data on behalf of Customer;
- **Supervisory Authority:** the competent independent data protection authority.

1.3. Data that Belco processes for its own independently determined purposes, such as billing, accounts receivable management, fraud prevention, contract administration and evidence of acceptance of legal documents, is not processing on behalf of Customer under this DPA. For such Processing, Belco is an independent Controller and Belco’s privacy notice applies.

2. Subject matter, application and order of precedence

2.1. This DPA governs Belco’s Processing of Customer Data in the performance of the Service. Details of the Processing are set out in Annex 1.

2.2. Customer determines the purposes and essential means of the Processing of Customer Data. Belco processes Customer Data solely for Customer and within the limits of Customer’s documented instructions, unless the Parties in fact have a different role for specific Processing.

2.3. The factual circumstances and the GDPR determine each Party’s role. A contractual qualification that does not correspond to the facts does not alter that statutory role.

2.4. In the event of a conflict concerning the Processing of Customer Data, the following order of precedence applies:

1. mandatory applicable data protection law;
2. applicable standard contractual clauses for international transfers;
3. this DPA, including its Annexes;

- 4. the Main Agreement;
- 5. other documentation.

2.5. This DPA does not give Belco the right to sell Customer Data or use it for Belco's own advertising, profiling for its own purposes or training of general-purpose AI models. Such Processing requires a separately documented role, legal basis and agreement.

2.6. Information is outside the scope of this DPA only when it has been anonymised in such a manner that identification of a natural person is no longer reasonably possible. Pseudonymisation alone is not anonymisation.

3. Documented instructions

3.1. Belco processes Customer Data solely:

- to provide, secure, maintain and support the Service in accordance with the Main Agreement;
- in accordance with the settings, roles, workflows, integrations and commands used by Customer in the Service;
- in accordance with additional written or electronically recorded instructions that fall within the agreed functionality and the law; and
- as further described in Annex 1.

3.2. The Main Agreement, this DPA, the configuration of the Service and demonstrable instructions given through the account or support channel together constitute Customer's documented instructions.

3.3. If Belco is required by Union or Dutch law to process Customer Data otherwise, Belco will inform Customer of that legal requirement before the Processing, unless the law prohibits such information on important grounds of public interest.

3.4. If Belco considers that an instruction infringes the GDPR or other applicable data protection law, Belco will inform Customer without undue delay. Belco may suspend the relevant instruction until Customer has confirmed or amended it, to the extent suspension is necessary to prevent a potential infringement.

3.5. An instruction outside the agreed Service or requiring disproportionate work will be carried out after consultation on feasibility, timing and reasonable costs. This provision does not limit Belco's statutory obligations.

4. Customer obligations

4.1. Customer is responsible for the lawfulness of the Processing of Customer Data and ensures that it:

- has a valid legal basis for the Processing and disclosure to Belco;
- informs Data Subjects correctly and in a timely manner;
- causes only Personal Data that is adequate, relevant and necessary to be processed;
- appropriately configures retention periods, access rights, integrations and other settings;
- issues instructions that comply with the GDPR;
- handles requests from Data Subjects and notifications to the Supervisory Authority; and
- carefully manages user accounts, roles, login credentials and connected external services.

4.2. Customer will not use the Service for systematic Processing of special categories of Personal Data, criminal-conviction data, national identification numbers or other exceptionally high-risk data unless this is necessary and lawful and the Parties have agreed appropriate additional measures in writing in advance. Incidental inclusion of such data in customer communications does not release either Party from its legal obligations.

4.3. Customer will prevent passwords, secret keys or full payment card details from being entered in free-text fields, messages or attachments, except where a specific part of the Service is expressly designed for that purpose.

5. Confidentiality and personnel

5.1. Belco ensures that persons acting under its authority who have access to Customer Data:

- receive access only to the extent necessary for their duties;
- process Customer Data only in accordance with Customer's instructions;
- are subject to contractual or statutory confidentiality obligations; and

- receive appropriate instruction on data protection and information security.

5.2. The confidentiality obligation continues after the end of the work or this DPA.

5.3. Belco manages access rights throughout the lifecycle of an account or role. Privileged access is restricted and controlled in accordance with Annex 2.

6. Security

6.1. Belco implements and maintains appropriate technical and organisational measures as referred to in Article 32 GDPR. Annex 2 describes the categories of measures Belco applies to the Service.

6.2. When determining appropriate measures, Belco takes into account the state of the art, the costs of implementation, the nature, scope, context and purposes of the Processing, and the risks of varying likelihood and severity for Data Subjects.

6.3. Belco may adapt the measures to technological developments and changed risks, provided that the overall level of protection is not materially reduced.

6.4. Customer acknowledges that security is a shared responsibility. Customer is responsible, among other things, for an appropriate role structure, timely revocation of accounts, secure endpoint devices, protection of login credentials, configuration of available security options and the security of integrations selected by Customer.

6.5. No security measure can prevent every incident. This does not affect Belco's obligation to demonstrably implement appropriate measures.

7. Personal Data Breaches

7.1. Belco will inform Customer without undue delay after becoming aware of a Personal Data Breach concerning Customer Data.

7.2. To the extent the information is available at the time, the notification will include:

- the nature of the Personal Data Breach;
- the categories and approximate number of Data Subjects concerned;
- the categories and approximate number of personal data records concerned;
- the likely consequences;
- the measures taken or proposed to end the Personal Data Breach and mitigate its consequences; and
- a contact point for further information.

7.3. If not all information is available at the same time, Belco will provide it in phases without further undue delay.

7.4. Belco will take reasonable measures to investigate and contain the Personal Data Breach and help prevent recurrence. Belco maintains an incident register to the extent required by the GDPR.

7.5. Customer decides whether notification to a Supervisory Authority or communication to Data Subjects is required. Taking into account the nature of the Processing and the information available, Belco will provide reasonable assistance with that assessment and notification. Belco will not notify on Customer's behalf without instructions unless required by law.

7.6. A notification or cooperation does not in itself constitute an admission of liability or breach of contract.

8. Data Subject rights

8.1. Taking into account the nature of the Processing, Belco will assist Customer by appropriate technical and organisational measures in fulfilling requests from Data Subjects, including access, rectification, erasure, restriction, portability and objection, to the extent those rights apply.

8.2. If a Data Subject contacts Belco directly about Customer Data, Belco will forward the request to Customer without undue delay and will not respond substantively except on Customer's instructions or where required by law.

8.3. Where Customer can fulfil a request independently through standard functionality, Customer will use that functionality first. Additional assistance outside standard functionality may, following prior consultation, be provided at reasonable cost, without prejudice to mandatory statutory obligations.

9. Assistance with compliance

9.1. Taking into account the nature of the Processing and the information available to Belco, Belco will provide reasonable assistance with Customer's compliance with Articles 32 through 36 GDPR, including:

- security of Processing;
- assessment and notification of Personal Data Breaches;
- a data protection impact assessment; and
- any prior consultation with a Supervisory Authority.

9.2. Upon reasonable request, Belco will provide information about the Service that Customer needs for its risk assessment or data protection impact assessment. Customer remains responsible for carrying out and documenting that assessment.

9.3. If the requested assistance materially exceeds the standard services, the Parties may agree reasonable costs and a schedule. This may not make legally required and time-critical assistance effectively impossible.

10. Subprocessors

10.1. Customer gives Belco general written authorisation to engage Subprocessors to perform the Service.

10.2. Belco maintains a current subprocessor register on the Legal Page. That register forms an integral part of this DPA and states, for each Subprocessor, at least the service used, the purpose of the Processing and, where relevant, information on international transfers.

10.3. Services actually used at the publication of version 2.0 are listed in Annex 3. The current online register governs later additions and replacements, subject to the notice and objection procedure in this Article.

10.4. Belco imposes on each Subprocessor in writing materially the same data protection obligations as apply to the relevant Processing under this DPA, including appropriate security, confidentiality, assistance, deletion and international-transfer requirements.

10.5. Belco remains fully responsible to Customer for the performance of its Subprocessors' obligations to the extent provided by Article 28(4) GDPR.

10.6. Belco will notify Customer directly, through the email address registered with the account and/or a clear notice in the Service, at least 30 days before adding or replacing a Subprocessor. If an expedited change is necessary to mitigate a serious security risk, ensure continuity or comply with the law, Belco will inform Customer as soon as possible and explain the reason for the shorter period.

10.7. Customer may object within 14 days after the notice on reasonable grounds directly related to the protection of Customer Data. The Parties will then consult in good faith on a reasonable solution. If no reasonable solution is available, Customer may terminate the demonstrably affected part of the Service or, where that part is material, terminate the Main Agreement in accordance with its procedure.

10.8. An external service that Customer selects, activates or connects and that acts directly under Customer's instruction or responsibility is not automatically a Subprocessor of Belco. The factual allocation of roles remains decisive.

10.9. Software that Belco runs on its own infrastructure without the software provider having access to Customer Data is not in itself a Subprocessor. The provider of the underlying infrastructure may be a Subprocessor and will in that case be included in the current register.

11. International transfers

11.1. Belco transfers Customer Data to a country outside the European Economic Area or to an international organisation only on the basis of a valid transfer mechanism under Chapter V GDPR.

11.2. A valid transfer mechanism may consist of an applicable adequacy decision of the European Commission, applicable standard contractual clauses of the European Commission or another safeguard permitted by law.

11.3. Where standard contractual clauses are used, Belco applies the module corresponding to the parties' factual roles. For a transfer from Belco as Processor to a Subprocessor, this will in principle be the processor-to-processor module.

11.4. Where required, Belco assesses the laws and practices of the third country and implements supplementary technical, contractual or organisational measures when necessary to ensure an essentially equivalent level of protection.

11.5. Belco relies on the EU–US Data Privacy Framework only where the relevant US recipient is validly certified for the relevant categories of data. If that mechanism ceases to apply, Belco will implement another valid safeguard before any further transfer or discontinue the transfer.

11.6. The current subprocessor register and Annex 4 describe how Belco manages international transfers. Belco does not make a general commitment that data remains exclusively within the EEA unless it expressly confirms this in writing for a specific service.

11.7. Where Customer itself activates an integration that results in a transfer outside the EEA, that activation constitutes a documented instruction for the technically necessary transfer. This does not release either Party from Chapter V GDPR. If Customer contracts directly with the external recipient, Customer is responsible for the transfer safeguard associated with its role. If Belco engages the recipient as a Subprocessor, Belco is responsible for the safeguard associated with its role.

12. Government requests

12.1. Belco will disclose Customer Data to a government authority only where legally required to do so.

12.2. To the extent legally permitted, Belco will inform Customer of the request before disclosure. If prior information is prohibited, Belco will inform Customer as soon as it lawfully can.

12.3. Belco will assess whether the request is valid, binding, specific and proportionate and will restrict the disclosure or challenge the request where reasonable legal grounds exist. Belco will not disclose more Customer Data than legally required.

13. Demonstrating compliance and audits

13.1. Belco will make available all information reasonably necessary to demonstrate compliance with Article 28 GDPR and this DPA.

13.2. Belco may initially use available independent assurance reports, certifications, summaries of security tests, questionnaires and other appropriate evidence. The absence of a certification does not automatically mean that Article 32 GDPR is not met.

13.3. If the available information is reasonably insufficient, Customer may conduct an audit itself or through an independent, qualified auditor. The following applies:

- Customer will normally give at least 30 days' written notice;
- the audit will normally take place during regular business hours and once per twelve-month period;
- the auditor is not a direct competitor of Belco and is bound by appropriate confidentiality;
- the audit is limited to systems, processes and information relevant to Customer Data;
- the audit does not unnecessarily disrupt the Service and protects data and confidential information of other customers; and
- the Parties will, where possible, use secure remote evidence before requesting on-site access.

13.4. The limitations in Article 13.3 do not apply to the extent a Supervisory Authority requires otherwise or where a Personal Data Breach, specific indication of material non-compliance or a legally urgent situation reasonably requires a faster or additional audit.

13.5. Customer bears its reasonable internal and external audit costs unless the audit reveals a material breach by Belco. In that case, Belco bears its own reasonable costs and the reasonable costs of the necessary follow-up audit. Financial arrangements may not make the statutory right of audit effectively impossible.

13.6. Belco will cooperate with investigations by the competent Supervisory Authority to the extent required by law.

14. Return, export and deletion

14.1. During the term, Belco provides Customer, within the available functionality, with means to access, export and delete Customer Data. Supported formats and limitations are described in the Service or product documentation.

14.2. After the end of the Processing services, Belco will, at Customer's choice, delete all Customer Data or return it to Customer, and delete existing copies, unless Union or Dutch law requires storage.

14.3. Customer will communicate its choice no later than upon termination. If Customer does not make a choice, Belco will delete Customer Data in accordance with its documented deletion process. Belco will inform Customer of the available export option before deletion becomes final.

14.4. Belco will carry out return and deletion without undue delay. Data in backups will be overwritten or deleted in accordance with the regular secure backup cycle and will remain protected from other use until then, except where necessary for recovery or required by law.

14.5. Data that must be retained by law will be restricted, used only for that legal purpose and deleted when the retention obligation ends.

14.6. Upon reasonable request, Belco will confirm in writing that deletion has been completed in accordance with this Article.

15. Term and termination

15.1. This DPA begins upon electronic acceptance and remains in force for as long as Belco processes Customer Data on Customer's behalf, including during a free trial.

15.2. Termination of the Main Agreement does not terminate this DPA while Belco continues to process or retain Customer Data.

15.3. Provisions that by their nature are intended to continue after termination, including confidentiality, audit concerning the relevant prior period, deletion, international transfers and liability, remain in effect for as long as necessary.

16. Electronic acceptance and evidence

16.1. This DPA may be entered into electronically in accordance with Article 28(9) GDPR. Acceptance may take place through a checkbox that is not pre-selected or through clear acceptance wording with links to the documents displayed directly next to the button used to start a trial, activate a paid account or confirm updated legal documents.

16.2. Within an existing organisation, acceptance may be completed by a user with the **owner** or **admin** account role. Customer is responsible for correctly assigning and timely revoking those roles. No separate authority declaration is required in the upgrade flow. Belco retains the available evidence of the authenticated action and, for a paid Subscription, the activation or payment.

16.3. For evidence and compliance purposes, Belco records the data that is available and necessary in the acceptance flow used. This may include:

- organisation ID and organisation name;
- user ID, name and email address as registered at the time of acceptance;
- date and time in UTC, recorded server-side;
- source event, such as `trial_signup`, `paid_upgrade` or `legal_update`;
- language, version number and document ID of the accepted Terms and Conditions and DPA;
- a cryptographic hash, document ID, publication archive or other reliable identification of the applicable documents;
- the acceptance text and button label displayed, where recorded; and
- IP address and, where proportionate, user agent or session ID.

16.4. Belco protects retained acceptance evidence against unauthorised alteration, restricts access and retains it no longer than necessary for contract evidence, legal obligations and the limitation or resolution of legal claims. Belco processes this evidence as an independent Controller in accordance with applicable privacy law.

16.5. Upon request, Customer may receive a copy of the accepted version and the acceptance details recorded for its organisation.

17. Amendments and notice

17.1. Belco may amend this DPA where necessary due to changes in law, instructions from supervisory authorities, changed Processing or a material change to the Service.

17.2. A substantive amendment will be notified directly to Customer at least 30 days before its intended effective date through the registered email address and/or a clear notice in the Service. The notice will include the new version, effective date and a comprehensible summary of the changes.

17.3. A substantively amended DPA will take effect for Customer only after an owner or admin has accepted it electronically, except where mandatory law requires earlier application. Publication on a website or continued use alone does not constitute approval of a substantively amended DPA.

17.4. If Customer does not accept the amended version before the announced date, the existing version continues to apply for as long as Belco can lawfully continue Processing under that version. If the amendment is necessary to continue providing the Service lawfully or securely, Belco may, after an additional reasonable period, suspend access to Processing or terminate the Main Agreement in accordance with its terms. Belco will first give Customer a reasonable opportunity to export Customer Data.

17.5. Article 17.3 does not apply to:

- a change in Subprocessors under Article 10, to which the general authorisation and objection procedure described there applies;
- an editorial correction without substantive effect; or
- a change to Annex 2 that does not materially reduce the overall level of protection.

17.6. Each published version receives a unique version number, effective date and immutable copy. Belco archives previous versions for evidentiary purposes.

17.7. Version 2.0 applies from the actual date of acceptance and is not backdated. Belco retains previous versions and existing acceptance records so that it can be established which version applied during which period.

18. Liability

18.1. The liability provisions of the Main Agreement apply to the extent permitted by law and not contrary to the GDPR.

18.2. Nothing in this DPA limits rights of Data Subjects or liability that cannot be contractually excluded or limited under Article 82 GDPR or other mandatory law.

18.3. Each Party is responsible for damage and costs arising from its own acts or omissions, in accordance with the factual allocation of roles and applicable law.

19. Contact and notices

19.1. Privacy and security notices to Belco must be sent to hello@belco.io.

19.2. Belco sends notices to the organisation's primary email address and/or to owners and admins in the Service. Customer keeps these details current.

19.3. A Personal Data Breach or urgent security incident will be reported through a channel clearly identifiable as such and not solely through a public web page.

20. Language, governing law and final provisions

20.1. Belco makes this DPA available in Dutch and English with the same version number and content. The Dutch version is the source document. If there is a difference in interpretation, the Dutch version prevails unless the Parties have expressly agreed in writing that the English version prevails. Mandatory law always takes precedence.

20.2. This DPA is governed by Dutch law. The dispute resolution provision in the Main Agreement also applies to this DPA, except where mandatory law or the competence of a Supervisory Authority provides otherwise.

20.3. If a provision is void, voidable or unenforceable, the remaining provisions remain in effect. The Parties will replace the relevant provision with a valid provision that most closely reflects its purpose and intent without limiting the GDPR.

20.4. A waiver of a right is valid only if made expressly and in writing and applies only to the specific case.

Annex 1 — Details of the Processing

1. Subject matter

Belco processes Customer Data to provide Customer with the Belco customer communication and customer service solution. Depending on the configuration selected by Customer, this may include:

- receiving, sending, routing, displaying, searching, labelling and retaining customer communications;
- collaborating on and handling conversations and tickets;
- managing contacts, users, teams, roles, tags, notes and workflows;
- connecting communication channels and external systems;
- displaying context from connected online stores or other sources;
- technical support, troubleshooting and recovery at Customer's request; and
- security, abuse detection, logging, backup and continuity of the Service.

2. Duration

The Processing lasts from the first moment Customer causes Customer Data to be processed in the trial or paid Service until the data has been returned or deleted in accordance with Article 14.

3. Nature and frequency

The Processing may consist of collection, recording, organisation, structuring, storage, adaptation, retrieval, consultation, use, transmission, making available, combination, restriction, export, archiving and deletion. It takes place continuously or on request for as long as Customer uses the relevant features.

4. Purposes

Belco processes Customer Data solely for:

1. providing the configured Service;
2. carrying out Customer's commands and workflows;
3. availability, integrity, confidentiality and recovery of the Service;
4. technical support and error analysis;
5. prevention and investigation of abuse and security incidents; and
6. compliance with a legal obligation directly applicable to Belco in accordance with Article 3.3.

Use for Belco's own marketing or training of general-purpose AI models is not included in these purposes.

5. Categories of Data Subjects

Depending on Customer's use, Customer Data may relate to:

- Customer's customers, former customers, prospects and leads;
- visitors to and users of Customer's websites, online stores, apps and communication channels;
- purchasers, recipients, return applicants and contacts associated with orders;
- Customer's employees, temporary staff, contractors, agents and account users;
- Customer's suppliers, business partners and other contacts; and
- persons who participate in or are mentioned in emails, chats, telephone calls, social messages or attachments.

6. Categories of Personal Data

Depending on what Customer enters or connects, the following categories may be processed:

- identification and contact details, such as name, company name, address, email address, telephone number, username and profile picture;
- account and authorisation data, such as organisation, role, teams, channel identifiers and external account IDs;
- communication content, such as emails, chat messages, social messages, WhatsApp messages, internal notes, any transcripts and attachments;
- order and customer-relationship data, such as order number, products, delivery, returns, status, amounts and customer history, to the extent available through an integration;
- telephony data, such as number, call time, duration and, only if activated and lawful, a call recording or transcript;
- technical and usage data, such as IP address, timestamps, browser or device characteristics, log data, error messages and audit events;
- labels, priorities, routing information, preferences and other metadata determined by Customer;
- authentication tokens or integration data required for a connected service to function; and
- special-category or criminal-conviction data incidentally included in free-form communications by Data Subjects or Customer, although the Service is not intended for systematic Processing of such data without additional arrangements.

Full payment card details are not intended Customer Data.

7. Retention

Customer Data is processed for as long as necessary to provide the Service, in accordance with the settings selected by Customer and applicable legal obligations. Operational logs, security logs, temporary support files and backups are retained only for as long as reasonably necessary for security, support, recovery and continuity. Following termination, Article 14 and the regular secure deletion cycles of Belco and its Subprocessors apply.

8. Customer's rights and obligations

Customer has the rights and obligations set out in the GDPR, the Main Agreement and this DPA. Customer may, among other things, issue instructions, manage settings, request information, conduct an audit, request export or deletion, and object to a new Subprocessor in accordance with the agreed procedures.

9. Additional instructions

Additional instructions are recorded through account settings, a support ticket, email or a document signed by the Parties. Belco will confirm oral instructions in writing before carrying them out, unless immediate action is necessary to mitigate an incident.

Annex 2 — Technical and organisational measures

Belco maintains a risk-based information security programme appropriate to the Service and the nature of Customer Data. Measures are reviewed periodically and following relevant changes or incidents.

1. Governance and risk management

Belco assigns responsibilities for information security and privacy and maintains policies and working procedures for access management, changes, incidents, backup, deletion and suppliers. Relevant risks, incidents and vulnerabilities are appropriately recorded, assessed and addressed.

2. Identity and access management

Belco uses individual accounts, role-based access and the principle of least privilege. Access rights are managed on onboarding, role changes and offboarding and are periodically reviewed based on risk. Privileged access is additionally restricted and, where appropriate and technically available, protected by multi-factor authentication.

3. Encryption and secrets

Belco protects Customer Data in transit using current, generally accepted secure protocols. Stored data, backups, keys, tokens and other secrets are protected using measures appropriate to the risk and infrastructure used. Passwords are not knowingly stored in readable form.

4. Segregation and minimisation

Belco applies logical separation between organisations and authorisation controls to organisation data. Production, test and development are separated by appropriate technical or organisational controls. Production data is not routinely used for development or testing and, where its use is necessary, is limited and anonymised or pseudonymised where possible.

5. Secure development and changes

Changes to the Service are developed, reviewed, tested and deployed through a controlled process proportionate to risk. Access to source code and deployment capabilities is restricted. Dependencies and relevant vulnerability notifications are assessed, and security-relevant defects are addressed based on risk.

6. Logging, monitoring and detection

Belco logs and monitors operational and security-relevant events to the extent appropriate for availability, error analysis, abuse detection and incident investigation. Access to logs is restricted, and their content and retention are aligned with necessity and risk.

7. Vulnerability and patch management

Belco assesses and addresses security updates and known vulnerabilities based on severity, exposure and risk. Publicly accessible components and critical dependencies are appropriately reviewed. Technical security tests are carried out with a scope and frequency appropriate to the risk.

8. Availability, backup and recovery

Belco uses backups or equivalent recovery facilities for data and configurations necessary for recovery. Access to recovery facilities is restricted. Recovery procedures are periodically tested or otherwise validated, taking into account the importance of the relevant systems.

9. Incident response

Belco maintains a procedure for detecting, classifying, containing, investigating, recovering from and evaluating security incidents. Relevant incidents are escalated internally, evidence is appropriately protected and corrective measures are followed up. Notifications to Customer are made in accordance with Article 7.

10. Personnel

Persons with access to Customer Data are subject to contractual or statutory confidentiality and receive security and privacy instructions appropriate to their roles. Access to systems and assets is changed or revoked on role changes and departure.

11. Supplier management

Belco assesses Subprocessors for relevant security, privacy and continuity risks and enters into appropriate written agreements. Critical suppliers are reassessed based on risk. On termination, access is revoked and data is deleted or returned in accordance with the agreements.

12. Physical security

For outsourced hosting, Belco also relies on the physical security measures of its infrastructure providers. Offices, workplaces and any local storage are protected by measures appropriate to the systems and information accessible there.

13. Deletion and media

Belco uses documented processes for deletion or irreversible overwriting. Data remaining only in secure backups remains subject to restricted access until overwritten or deleted through the regular cycle. Temporary support files and exports are deleted when no longer needed.

14. Continuous improvement

Belco may replace measures with technically or organisationally equivalent or better measures. Findings from incidents, tests, audits, supplier assessments and changed risks are used to improve the security programme.

Annex 3 — Current subprocessor register

Belco maintains the current subprocessor register on the Legal Page. That online register is authoritative and is amended in accordance with Article 10. Not every service below is used for every Customer or feature; a service is a Subprocessor only to the extent that it actually processes Customer Data on Belco's behalf.

At the publication date of version 2.0, the following services may be used in the Processing of Customer Data, depending on the enabled features and technical route:

Service	Function	International transfer
Scalingo	Production hosting, applications and databases	Primary hosting in the EEA
Amazon Web Services	Cloud infrastructure and storage components, where used	EEA and/or third countries; Article 11 applies
DigitalOcean	Production AMQP, workflow and infrastructure components, where used	EEA and/or third countries; Article 11 applies
Cloudflare	DNS, CDN, security and internet-traffic transmission	Global network; Article 11 applies where required
Mailgun / Sinch	Transactional email and delivery metadata	EEA and/or third countries; Article 11 applies
Twilio	Communication and telephony services	EEA and/or third countries; Article 11 applies
360dialog	WhatsApp Business platform and message traffic	Depends on the selected WhatsApp route; Article 11 applies where required
Speakup	Telephony, number and traffic data	Primarily EEA; Article 11 applies where required
Axeos	Telephony platform and licence components, to the extent data is processed	Depends on the activated telephony route
WotNot	Chatbot and AI functionality, where activated by Customer	EEA and/or third countries; Article 11 applies
Pushwoosh	Push notifications and device identifiers, where used	EEA and/or third countries; Article 11 applies
Monti APM	Application performance monitoring, to the extent logs contain Customer Data	EEA and/or third countries; Article 11 applies
Bunny.net	CDN and cloud storage, where used	Global network; Article 11 applies where required
ip-api / Artia International	IP geolocation, where activated	EEA and/or third countries; Article 11 applies where required

Another supplier is considered a Subprocessor only if and to the extent it actually processes Customer Data on Belco's behalf. Belco will add such a supplier to the current register before or when that Processing begins and will apply the notice and objection procedure in Article 10.

Annex 4 — International transfers

1. Principle

Belco processes Customer Data within or outside the EEA only in accordance with Article 11. For a relevant Subprocessor, the current subprocessor register states whether an international transfer may take place and the type of safeguard used.

2. Assessment and safeguards

For a relevant transfer, Belco records as applicable:

- the parties involved and their roles;
- the categories of data and Data Subjects;
- the purpose and frequency of the transfer;
- the countries of storage or access;
- the applicable transfer mechanism;
- necessary supplementary technical, contractual or organisational measures; and
- the result and reassessment of a transfer impact assessment where required.

3. Standard contractual clauses

Where Belco uses standard contractual clauses, the applicable clauses of the European Commission are incorporated by reference into the arrangements with the relevant recipient. In the event of a conflict concerning the international transfer, those standard contractual clauses prevail.

4. Change or lapse of a safeguard

Belco monitors, to the extent reasonably possible, the validity of the transfer safeguards used. If an adequacy decision, certification, standard contractual clause or other safeguard is no longer valid or sufficient, Belco will discontinue the relevant transfer or implement a valid replacement safeguard without undue delay. Belco will inform Customer where the change is material.