

Verwerkingsregister | CAO Platform

Laatste update: 9 juli 2026

1. Inleiding

Dit register bevat een overzicht van categorieën verwerkingen van persoonsgegevens die CAO Platform verricht als verwerker namens klanten in de zin van artikel 30 AVG. Het register heeft een intern karakter en ziet op categorieën verwerkingsactiviteiten, niet op afzonderlijke klantdossiers. Het doel van dit register is om op gestructureerde wijze inzicht te geven in de aard en inrichting van de verwerkingen die CAO Platform namens zijn klanten uitvoert.

2. Gegevens van de verwerker

CAO Platform is een handelsnaam van Jaclang CAO-Online, gevestigd aan De Stelling 10-49, 8232 EB te Lelystad, ingeschreven in het Handelsregister onder KvK-nummer 32129292. Er is geen functionaris voor gegevensbescherming aangesteld omdat CAO Platform daartoe niet wettelijk verplicht is.

3. Categorieën verwerkingsverantwoordelijken

De verwerkingsverantwoordelijken namens wie CAO Platform persoonsgegevens kan verwerken, kunnen onder meer bestaan uit werkgevers, transportbedrijven, administratiekantoren, salarisverwerkers, accountants, softwareleveranciers, leveranciers van boordcomputers, leveranciers van TMS-systemen en overige zakelijke organisaties die gebruikmaken van één of meerdere onderdelen van het platform.

4. Algemene beschrijving van de verwerkingen als verwerker

CAO Platform kan namens klanten persoonsgegevens verwerken in het kader van het beschikbaar stellen, hosten, uitvoeren, onderhouden, beveiligen en ondersteunen van het platform en de daaraan verbonden modules, koppelingen, supportomgevingen en overige digitale voorzieningen. Daarbij kan CAO Platform persoonsgegevens ontvangen, opslaan, structureren, combineren, verrijken, exporteren, importeren, synchroniseren, rapporteren, archiveren, beveiligen en anderszins verwerken voor zover dat noodzakelijk is voor de uitvoering van de overeenkomst met de betreffende klant.

5. Algemene beschrijving van technische en organisatorische beveiligingsmaatregelen

CAO Platform treft passende technische en organisatorische maatregelen, waaronder waar passend toegangsbeperking, gebruikersrechten, authenticatie, logging, beveiligde verbindingen, back-ups, geheimhoudingsverplichtingen en organisatorische controlemaatregelen. Deze maatregelen worden afgestemd op de aard van de verwerkingen en de risico’s voor betrokkenen.

6. Overzicht van categorieën verwerkingen

Nr	Categorie verwerking	Categorieën verwerkingsverantwoordelijken	Categorieën betrokkenen	Categorieën persoonsgegevens	Aard en doel van de verwerking	Ontvangers / subverwerkers / systemen	Doorgifte buiten EER	Algemene bewaarlijn	Beveiligingsmaatregelen
1	Platformaccounts en gebruikersbeheer	Klanten die accounts en gebruikers binnen het platform beheren.	Gebruikers, beheerders en contactpersonen van klanten.	Gebruikersnamen, e-mailadressen, autorisaties, gebruikersrollen, accountinstellingen, herstelgegevens en toegangsgegevens.	Het aanmaken, beheren, autoriseren, beveiligen en ondersteunen van bedrijfsaccounts en gebruikersaccounts.	Hosting- en infrastructuurleveranciers, IT-dienstverleners en andere subverwerkers voor zover noodzakelijk.	Nee	Zolang noodzakelijk voor de uitvoering van de overeenkomst en daarna conform klantafspraken of wettelijke bewaarplichten.	Authenticatie, toegangsbeperking, logging, beveiligde verbindingen en afgeschermd beheeromgevingen.
2	CAO-, loon- en arbeidsvoorwaardelijke gegevens	Werkgevers, administratiekantoren, salarisverwerkers en overige zakelijke klanten.	Werknemers, chauffeurs, uitzendkrachten, contactpersonen en gebruikers.	Arbeidsgegevens, functiegroepen, dienstverbandgegevens, looncomponenten, toeslagen, roosters, uren en cao-gerelateerde gegevens.	Berekenen, controleren, toepassen en administreren van cao- en arbeidsvoorwaardelijke aanspraken.	Salarissoftware, administratiesystemen, rapportagetools en ondersteunende IT-leveranciers.	Nee	Volgens instructies van de klant en zolang nodig voor administratie, controle en wettelijke verplichtingen.	Autorisatiebeheer, logging, versleutelde verbindingen, back-ups en rolgebaseerde toegang.
3	Koppelingen met externe systemen	Klanten die koppelingen gebruiken met boordcomputers, TMS-, HR- of salarissystemen.	Werknemers, chauffeurs, planners, gebruikers en contactpersonen .	Identificatiegegevens, arbeidsgegevens, planningsgegevens, urenregistraties, rit- en taakgegevens en systeem-ID's.	Importeren, exporteren, synchroniseren en controleren van gegevens tussen het platform en externe systemen.	Boordcomputerleverancier s, TMS-leveranciers, salaris- en HR-systemen, API- en hostingpartijen.	Afhankelijk van de door de klant gekozen externe systemen.	Conform klantinstructie en zolang noodzakelijk voor koppeling, controle en foutafhandeling.	Beveiligde API's, toegangsbeheer, logging, versleuteling en technische scheiding van klantomgevingen.
4	Rapportages, controles en exports	Klanten die rapportages, controles of exports uit het platform genereren.	Werknemers, chauffeurs, gebruikers en contactpersonen .	Rapportagegegevens, arbeids- en urengegevens, controlebevindingen, exportbestanden en metadata.	Genereren van overzichten, controles, audits, exports en managementinformatie voor klanten.	Rapportagetools, exportvoorzieningen, opslaglocaties en eventueel klantgebonden systemen.	Nee	Zolang noodzakelijk voor rapportage, controle en eventuele herstel- of auditdoeleinden.	Autorisaties, logging, beveiligde opslag, exportbeperkingen en organisatorische controle.
5	Support, beheer en klantondersteuning	Klanten die ondersteuning, beheer of technische hulp ontvangen.	Gebruikers, beheerders, contactpersonen en eventueel werknemers over wie vragen worden gesteld.	Contactgegevens, accountgegevens, supportvragen, foutmeldingen, schermafbeeldingen, loggegevens en relevante dossierinformatie.	Beantwoorden van vragen, oplossen van incidenten, uitvoeren van onderhoud en ondersteunen van klanten.	Ticketsystemen, e-mail, beheeromgevingen, hostingpartij en IT-dienstverleners.	Nee	Zolang noodzakelijk voor support, incidentafhandeling, kwaliteitscontrole en klantafspraken.	Autorisatie, logging, geheimhouding, beperkte toegang en beveiligde communicatiekanalen.
6	Hosting, opslag en back-ups	Alle klanten die gebruikmaken van het platform of daaraan gekoppelde diensten.	Alle betrokkenen van wie gegevens via het platform worden opgeslagen.	Platformgegevens, klantgegevens, gebruikersgegevens, logbestanden, configuratiegegevens en back-upgegevens.	Beschikbaar stellen, hosten, beveiligen, herstellen en continueren van het platform en de dienstverlening.	Hostingprovider, datacenters, back-upleveranciers en technische beheerpartijen.	Nee	Zolang nodig voor dienstverlening, continuïteit, herstel en naleving van klantafspraken.	Datacenterbeveiliging, back-ups, toegangscontrole, versleuteling, monitoring en continuïteitsmaatregelen.
7	Logging, monitoring en beveiliging	Alle klanten binnen de platformomgeving.	Gebruikers, beheerders en technische contactpersonen .	Loggegevens, IP-adressen, gebruikers-ID's, tijdstippen, acties, foutmeldingen en beveiligingsmeldingen .	Bewaken van beveiliging, beschikbaarheid, foutopsporing, misbruikpreventie en incidentonderzoek.	Monitoringtools, loggingdiensten, hostingpartij en beveiligingsleveranciers.	Nee	Zolang noodzakelijk voor beveiliging, foutanalyse, incidentafhandeling en bewijsvoering.	Loggingbeperking, toegangscontrole, monitoring, incidentprocedures en beveiligde opslag.
8	Test-, acceptatie- en ontwikkelomgevingen	Klanten van wie gegevens of configuraties worden gebruikt voor testen of ontwikkeling, voor zover noodzakelijk.	Gebruikers, werknemers, chauffeurs en contactpersonen , voor zover testgegevens	Testgegevens, configuraties, voorbeeldbestanden, foutmeldingen, loggegevens en eventueel	Ontwikkelen, testen, controleren, verbeteren en accepteren van functionaliteiten en koppelingen.	Ontwikkeltools, testomgevingen, hostingpartij en softwareontwikkelaars.	Nee	Zo kort mogelijk en conform testdoel, klantinstructie en interne verwijderafspraken .	Afscherming, pseudonimisering waar mogelijk, beperkte toegang, logging en scheiding van omgevingen.

			persoonsgegevens bevatten.	afgeschermd productiegegevens.					
9	Migratie, import en inrichting	Nieuwe of bestaande klanten bij inrichting, conversie, migratie of import van gegevens.	Gebruikers, werknemers, chauffeurs, contactpersonen en overige betrokkenen uit aangeleverde bestanden.	Importbestanden, identificatiegegevens, arbeidsgegevens, accountgegevens, configuraties en migratielogbestanden.	Inrichten van klantomgevingen, migreren, converteren, valideren en importeren van gegevens.	Importtools, migratiesoftware, hostingpartij, klantensystemen en betrokken IT-dienstverleners.	Nee	Zolang nodig voor inrichting, validatie, herstel en afronding van de migratie of import.	Beveiligde aanlevering, toegangsbeperking, logging, gecontroleerde verwijdering en scheiding van klantdata.

7. Slotopmerking

Dit register wordt aangepast indien de categorieën verwerkingen, de categorieën verwerkingsverantwoordelijken, de gebruikte systemen, de categorieën persoonsgegevens, de ontvangers of de toepasselijke wet- en regelgeving daartoe aanleiding geven.