Civinc beveiligingsbeleid

Versie 2.0 · Geldig vanaf 29-7-2026 · Jaarlijks herzien

Dit document beschrijft de technische en organisatorische maatregelen die wij treffen op grond van artikel 32 AVG. Het maakt deel uit van onze verwerkersovereenkomst. Waar dit document en die overeenkomst van elkaar afwijken, gaat de overeenkomst voor.

1. Wat wij beschermen, en hoe weinig dat is

De sterkste beveiligingsmaatregel is de gegevens niet verzamelen. Civinc vraagt deelnemers nooit om een naam, e-mailadres, telefoonnummer of andere informatie die naar hun persoonlijke identiteit leidt. Sessiegegevens zijn gekoppeld aan een willekeurig gegenereerde identificatiecode, en wij beschikken niet over een sleutel die die code aan een persoon koppelt. Een inbreuk op onze systemen zou niet onthullen wie wat heeft gezegd, omdat wij dat niet weten.

Gespreksinhoud is het gevoeligste gegeven dat wij bewaren, en wij bewaren het het kortst: het wordt binnen 72 uur na afloop van een sessie permanent verwijderd. Geen enkele medewerker van Civinc heeft er op enig moment toegang toe.

2. Mensen en toegang

- Toegang tot de achterliggende systemen met gebruikersgegevens is beperkt tot medewerkers op directieniveau. Niemand anders heeft die toegang, en zij wordt alleen verleend waar de functie dat vereist.
- Iedereen met die toegang is gebonden aan een schriftelijke geheimhoudingsverplichting die doorloopt na afloop van het dienstverband.
- Toegangsrechten worden ingetrokken en inloggegevens ongeldig gemaakt als onderdeel van ons uitdiensttredingsproces.
- Toegangsniveaus in alle systemen worden ten minste eenmaal per jaar beoordeeld.
- Beheeraccounts op onze eigen systemen en op die van onze leveranciers zijn beveiligd met meerfactorauthenticatie.
- Wachtwoorden en API-sleutels worden bewaard in een beheerde sleutelkluis, nooit in broncode, en worden bij personeelswisselingen vervangen.

3. Infrastructuur

Civinc draait volledig op Google Cloud Platform, op servers in de Europese Unie. Wij beheren geen eigen servers.

- Alle gegevens worden tijdens verzending versleuteld via HTTPS/TLS en in rust versleuteld opgeslagen.
- Klantgegevens zijn logisch gescheiden.
- Wij gebruiken Firebase App Check, dat controleert of aanroepen naar onze back-end afkomstig zijn van onze eigen applicatie en niet van een derde partij.
- Google Cloud beschikt over ISO 27001-, ISO 27017-, ISO 27018- en SOC 1-, 2- en 3-certificering en voert doorlopend penetratietests uit op de eigen infrastructuur.

Die certificaten dekken de infrastructuur waarop wij bouwen, niet onze eigen organisatie. Het volgende hoofdstuk beschrijft waar Civinc zelf staat.

4. Certificering

Civinc beschikte tot juni 2026 over ISO 27001-certificering. Wij hebben besloten die niet te verlengen om haalbaarheidsredenen die samenhangen met onze omvang als kleine onderneming. Wat wij hebben behouden is het managementsysteem dat onder het certificaat lag. Onze processen voor toegangsbeheer, leveranciersbeheer,

incidentafhandeling, risicobeoordeling en jaarlijkse evaluatie zijn de processen die wij hebben opgezet om aan ISO 27001 te voldoen, en die zijn nog steeds in werking. Ze worden in dit document beschreven.

5. Omgang met gegevens en bewaartermijnen

Gegevens	Bewaartermijn	Bescherming
Gespreksinhoud	Maximaal 72 uur na de sessie	Versleuteld opgeslagen, geen toegang voor medewerkers, permanent verwijderd. Uitsluitend bewaard zodat een deelnemer zijn gesprek kan terugkrijgen na het verversen van de pagina en zodat een eventuele AI-analyse kan draaien.
Antwoorden en sessie-metadata	Looptijd van de klantovereenkomst, maximaal drie jaar	Gepseudonimiseerd. Eerder verwijderd op instructie van de klant.
Beheeraccounts	Looptijd van de klantovereenkomst	Uitsluitend naam, e-mailadres en organisatie.
IP-adressen	Niet opgeslagen door Civinc	Verwerkt door Firebase om de verbinding tot stand te brengen; Civinc heeft er geen toegang toe.

Verwijdering is permanent en werkt binnen dezelfde cyclus door in back-ups. Bij beëindiging van een klantovereenkomst verwijderen of retourneren wij binnen dertig dagen alle gegevens van die klant, naar keuze van de klant.

6. AI-verwerking

Wanneer een klant AI-analyse inschakelt, worden gespreksfragmenten verstuurd naar Mistral AI SAS, een Frans bedrijf, en verwerkt op servers in de Europese Unie. Mistral treedt op als onze verwerker onder een verwerkersovereenkomst.

- Fragmenten worden losgekoppeld van de sessiecontext en geïsoleerd van alle andere gegevens. Mistral ontvangt niet de sessie als geheel, niet de identiteit van de klant en niet de gebruikerscode.
- Gegevens die naar Mistral gaan worden niet gebruikt om de modellen te trainen. Deze opt-out is ingesteld op organisatieniveau.
- Experimentele modellen (“Labs”) zijn uitgeschakeld, omdat die training toestaan ongeacht die opt-out.
- Wij gebruiken de feedback-endpoints niet, omdat die ingezonden inhoud buiten de opt-out zouden plaatsen.
- Mistral bewaart fragmenten maximaal 30 dagen voor het tegengaan van misbruik, waarna ze permanent worden verwijderd.

AI-analyse is per sessie optioneel, en de analyse draait pas wanneer er voldoende berichten zijn verstuurd over voldoende afzonderlijke gesprekken om een individuele bijdrage niet meer te kunnen onderscheiden. De uitkomst bevat nooit letterlijke citaten.

7. Veilige ontwikkeling

Beveiliging is een vast onderdeel van ons ontwikkelproces.

- Codeconventies worden automatisch afgedwongen via statische code-analyse.
- Wij gebruiken gevestigde frameworks die beschermen tegen veelvoorkomende aanvalstypen, waaronder XSS, CSRF en injectie.
- Continue integratie met unit- en integratietests; elke release wordt getest voordat die in productie komt.
- Afhankelijkheden worden doorlopend gemonitord en actueel gehouden; beveiligingsmeldingen worden opgevolgd zodra ze binnenkomen.
- Doorlopende kwetsbaarhedenscans met daarvoor bestemde tooling van derden.

- Wijzigingen worden door een collega beoordeeld voordat ze worden samengevoegd.

8. Monitoring, back-ups en continuïteit

- Toegang tot productiesystemen en beheerhandelingen worden gelogd.
- Back-ups worden gemaakt volgens vooraf vastgestelde frequenties.
- Omdat gespreksinhoud binnen 72 uur wordt verwijderd, komt die door dat ontwerp niet voor in oudere back-ups.

9. Incidenten en datalekken

Beveiligingsincidenten kunnen op elk moment en door iedereen worden gemeld via hello@civinc.co. Meldingen komen rechtstreeks bij onze CTO terecht.

- Elk incident wordt gedocumenteerd, beoordeeld en voorzien van een actieplan met beperkende maatregelen.
- Wanneer een datalek een klant raakt, informeren wij die klant zonder onnodige vertraging en in elk geval binnen 48 uur nadat wij ervan op de hoogte zijn geraakt, met de gegevens die artikel 33 lid 3 AVG voorschrijft.
- Wij melden niet namens een klant bij een toezichthouder of bij betrokkenen, tenzij daartoe schriftelijk opdracht is gegeven, omdat die beslissing bij de verwerkingsverantwoordelijke ligt.
- Wanneer personen rechtstreeks worden geraakt en bereikbaar zijn, benaderen wij hen via het passende kanaal.
- Na afhandeling evalueren wij wat er is gebeurd en wat er moet veranderen.

10. Subverwerkers

Leverancier	Entiteit en locatie	Rol
Google Cloud Platform	Google Cloud EMEA Ltd, EU-regio	Hosting, opslag, database en analyse-infrastructuur.
Google Firebase	Google Cloud EMEA Ltd, EU-regio	Verbinding tussen het apparaat van de deelnemer en het platform.
Mistral AI	Mistral AI SAS, Parijs, Frankrijk	AI-analyse van gespreksfragmenten, wanneer de klant die heeft ingeschakeld.

Elke subverwerker is gebonden aan een schriftelijke overeenkomst met gegevensbeschermingsverplichtingen die niet minder beschermend zijn dan de onze. Wij informeren klanten voordat wij een subverwerker toevoegen of vervangen, zodat zij bezwaar kunnen maken.

Gegevens worden opgeslagen binnen de EER. Onze hostingleverancier maakt deel uit van een groep met entiteiten buiten de EER waarvan medewerkers op afstand toegang kunnen hebben voor ondersteuning en onderhoud. Volgens de richtsnoeren van de EDPB is die toegang een doorgifte, en zij is gedekt door het EU-U.S. Data Privacy Framework met modelcontractbepalingen als terugvaloptie. Onze AI-leverancier verwerkt uitsluitend binnen de Europese Unie.

11. Evaluatie

Activiteit	Frequentie
Toegang tot systemen, hardware en documenten intrekken	Bij uitdiensttreding
Toegangsniveaus in alle systemen en voor alle medewerkers beoordelen	Jaarlijks
Dit beleid en de lijst met subverwerkers herzien	Jaarlijks en bij elke wezenlijke wijziging
Kritieke bibliotheken en afhankelijkheden actueel houden	Doorlopend
Unit- en integratietests	Doorlopend

Activiteit	Frequentie
Externe kwetsbaarhedenscans	Doorlopend

Vragen over dit beleid: hello@civinc.co