

AVG-proof lokale AI voor Greenvox

Interne voorbereiding voor de call van vandaag (15:00). Dit verslag is research, geen juridisch advies. De juridische kant moet altijd nog door een privacy-jurist of de FG getoetst worden.

Waar gaat het over

Greenvox wil een **AI-assistent voor klantmanagers**.

- Doel: admin ontzorgen + klantcontact met nagebootste schrijfstijl.
- Probleem: ze werken met **bijzondere persoonsgegevens** (UWV-data, re-integratie).
- Harde eis van Hamza (hun IT'er): **AVG-proof** en **geen data naar Amerikaanse cloud** (Claude, OpenAI).
- Voorkeur: een **lokaal open model** (Ollama/Llama/Mistral).

Dit verslag geeft 3 dingen:

1. Hoe EU/NL-bedrijven dit oplossen zonder US-cloud.
 2. De juridische kant (AVG bij bijzondere data).
 3. Een concrete, verantwoorde architectuur voor Greenvox.
-

1. Hoe los je dit op zonder Amerikaanse cloud?

Er zijn grofweg **drie routes**. Je kunt ze ook combineren.

Route A — Lokaal / on-premise (op eigen server)

Dit is de meest privacy-veilige optie.

- Je draait een **open model** op je eigen hardware.
- Tools: **Ollama**, **llama.cpp** of **vLLM** (vLLM is beter voor meerdere gebruikers tegelijk).
- Modellen: **Llama 3.3**, **Mistral** (Frans/EU), **Qwen**, **Gemma**.

- De data **verlaat het netwerk niet**. Geen US-cloud, geen training door derden.
- Dit heet "**privacy by design**": de bescherming zit ingebouwd, niet achteraf geplakt.

Een bron noemt dit letterlijk: een lokaal model dat op `localhost` draait, **stuurt tijdens gebruik niets naar buiten**. Dat is precies wat je wilt voor UWV-data.

Hardware (indicatie uit research):

- Instap (24 GB+ GPU): ruwweg **1.500–4.000 dollar**.
- Productie-server: **15k–25k dollar**.
- Break-even tegenover dure cloud-API's: vaak **6–12 maanden** bij veel gebruik.

Route B — EU-cloud (Europees gehost, geen US-bedrijf)

Wil je geen eigen server beheren? Dan kan een **Europese cloud**.

- **OVHcloud** (Frans) — heeft "AI Endpoints": EU-hosting, **zero data retention**, traint niet op je prompts.
- **Scaleway** (Frans) — "Generative APIs": Europese hosting, zero data retention.
- **Hetzner** (Duits) — kale servers in de EU, geschikt om zelf een model op te draaien.
- Mistral biedt zelf ook een **EU-API met een verwerkersovereenkomst (DPA)**.

Belangrijk: deze partijen vallen **niet** onder de Amerikaanse **CLOUD Act**. Dat is juist het hele punt.

Route C — Microsoft EU Data Boundary (let op: nuance)

Microsoft heeft sinds **februari 2025** de "EU Data Boundary" af.

- Data van EU-klanten wordt binnen de **EU/EFTA** opgeslagen en verwerkt.
- **Maar:** Microsoft blijft een **Amerikaans bedrijf** en valt onder de **CLOUD Act**.
- Voor Greenvox' harde eis ("geen Amerikaanse diensten") is dit **niet ideaal**.
- Noem het in de call als optie, maar Route A of B past beter bij hun eis.

2. De juridische kant (AVG bij bijzondere data)

Let op: **bijzondere persoonsgegevens** (gezondheid, re-integratie) zijn **extra zwaar beschermd** onder **AVG artikel 9**. Dat verandert de spelregels.

DPIA — bijna zeker verplicht voor Greenvox

Een **DPIA** (Data Protection Impact Assessment) is een verplichte privacy-toets vóóraf.

- De **Autoriteit Persoonsgegevens (AP)** noemt **re-integratiebedrijven** letterlijk als voorbeeld van organisaties die bij grootschalige gezondheidsdata een DPIA moeten doen.
- Greenvox = re-integratie + ~16.000 kandidaten + UWV-data = **grootschalig + bijzondere data**.
- De AP gebruikt 9 criteria; bij **2 of meer** is een DPIA verplicht. Greenvox raakt er meerdere (bijzondere data, grote schaal, evt. profilering).

Conclusie: een DPIA is hier vrijwel zeker verplicht. Doe die vóór je live gaat. Dit is ook je beste bewijs richting liability.

Grondslag (waarom mag je dit verwerken?)

- Voor bijzondere data heb je een **uitzondering op artikel 9** nodig (alleen "gerechtvaardigd belang" is hier meestal **niet genoeg**).
- Re-integratie loopt vaak via een **wettelijke taak / wettelijke verplichting** of expliciete toestemming.
- Dit moet **per verwerking** vastgelegd en getoetst worden.

Verwerkersovereenkomst

- Schakel je een externe partij in (bv. EU-cloud), dan is een **verwerkersovereenkomst verplicht** (AVG art. 28).
- Daarin staat: welke gegevens, hoe lang bewaard, welke beveiliging, en of er **subverwerkers** zijn.
- Bij een **volledig lokaal model** (Route A) heb je hier eigenlijk **geen verwerker** — dat is juist een groot voordeel.

Maatregelen die je aantoonbaar neemt

- **Privacy by design & by default** — bescherming ingebouwd vanaf het ontwerp.
- **Dataminimalisatie** — alleen verwerken wat echt nodig is.

- **Pseudonimisering / anonimisering** — namen en BSN eruit halen vóór het model ze ziet.
- **Versleuteling** — data versleuteld opslaan en versturen.
- **Toegangsbeveiliging** — alleen de juiste mensen erbij.
- **Bewaartermijnen** — niet langer bewaren dan nodig (re-integratiedossiers: vaak **minimaal 5 jaar**, check per dossier).
- **Logging** — vastleggen wat het systeem doet (ook nuttig voor de AI Act).

Het US-transfer-probleem (Schrems II)

- Sinds **Schrems II (2020)** is doorgifte naar de VS juridisch risicovol.
- Het **EU-VS Data Privacy Framework (DPF)** is de huidige opvolger.
- In **september 2025** hield het DPF stand bij de eerste rechtszaak, **maar** er loopt een **hoger beroep** bij het Europese Hof. De toekomst is dus **onzeker**.
- Daarom: voor bijzondere data is **niet afhankelijk willen zijn van de VS een verstandige keuze**. Greenvox' eis is juridisch goed te verdedigen.

Extra: EU AI Act (recruitment = hoog risico)

Let op, dit speelt ook mee:

- Onder de **EU AI Act** valt **werving & selectie expliciet onder "hoog risico"**.
- Verplichtingen: risicobeheer, **menselijk toezicht**, logging, technische documentatie, accuraatheid.
- De hoofddatum was **2 augustus 2026**, maar er ligt een voorstel (Digital Omnibus) om de hoog-risico-eisen **uit te stellen tot eind 2027**. Status: nog niet definitief.
- Boetes kunnen oplopen tot **35 miljoen euro of 7% wereldwijde omzet**.
- Praktisch: zorg dat een **mens altijd de eindbeslissing en de tekst controleert**. De AI is assistent, geen beslisser.

3. Concrete conclusie voor Greenvox

Aanbevolen architectuur (verantwoord + klein beginnen):

1. **Lokaal open model** (Ollama of vLLM met Llama 3.3 of Mistral) op een **eigen server** of bij een **EU-cloud** (OVHcloud/Scaleway/Hetzner). Geen US-cloud.
2. **Pseudonimiseer** de data vóór het model: haal namen, BSN en directe identifiers eruit.
3. **Begin klein** met één veilige taak — bijvoorbeeld **concept-teksten** in de schrijfstijl van de klantmanager, die de mens daarna **zelf controleert en verstuurt**. Niet meteen alles automatiseren.
4. **Mens in de lus**: AI stelt voor, mens beslist. Dit dekt zowel AVG als AI Act af.

Wat je aantoonbaar regelt (voor liability — dit is je dossier):

- **DPIA** uitvoeren vóór livegang (vrijwel zeker verplicht).
- **Verwerkersovereenkomst** met elke externe partij (of geen verwerker bij volledig lokaal).
- **Logging** van wat het systeem doet.
- **Grondslag** per verwerking vastleggen (art. 9-uitzondering).
- **Bewaartermijnen en toegangsbeveiliging** documenteren.
- Alles laten **toetsen door een privacy-jurist / FG** vóór livegang.

Kort voor Hamza: ja, het kan AVG-proof zonder US-cloud. De veiligste route is een **lokaal of EU-gehost open model + pseudonimisering + DPIA + mens in de lus**. Klein beginnen, alles documenteren.

Aanvulling (Hermes-check)

Extra punten uit een tweede controleronde, vlak voor de call. Vul de bovenstaande conclusie aan, vervangt niets.

1. FRIA naast DPIA (niet vergeten)

Bij **hoog-risico werving** onder de EU AI Act (art. 27) moet de gebruiker — de **deployer**, dus straks Greenvox — **naast de DPIA ook een FRIA** doen.

- **FRIA** = Fundamental Rights Impact Assessment, een **grondrechten-toets**.
- Het is een **andere toets** dan de DPIA: de DPIA kijkt naar privacy, de FRIA naar grondrechten breder (gelijke behandeling, non-discriminatie).

- **Noem ze allebei** in de call. Twee toetsen, geen keuze tussen de twee.

2. Schrijfstijl-nabootsing = transparantie-risico

Het nabootsen van de schrijfstijl van een klantmanager raakt de **transparantieplicht**.

- Denkt de klant dat een **mens** het bericht schrijft, terwijl het AI is? Dan geldt een **transparantieplicht**.
- **Oplossing**: een mens **keurt elk bericht en verstuurt het zelf** (mens-in-de-lus). De AI levert een concept, de mens neemt het over.
- Zo blijft het eerlijk én juridisch verdedigbaar.

3. Trainen vs RAG (belangrijk verschil)

NIET fijntrainen op de 16.000 kandidaat-profielen.

- Bij fijntrainen zit de data **in het model** verwerkt. Een **recht op vergetelheid** (een kandidaat die wil dat zijn data weg is) is dan **heel lastig** — je krijgt de data er niet zomaar weer uit.
- **Veiliger: RAG** (Retrieval Augmented Generation). Het model **leest de data alleen live op het moment** dat het nodig is, en **traint er niet op**.
- Data blijft in een aparte, beheersbare database. Verwijderen kan gewoon.

4. Single point of failure (1 lokale machine)

Eén lokale machine is privacy-veilig, maar **ook een risico** als hij uitvalt of gestolen wordt.

- **Versleutelde schijf** — bij diefstal is de data onleesbaar.
- **Fysieke beveiliging** — de machine in een afgesloten ruimte.
- **Back-upplan** — wat als de machine kapotgaat? Zorg voor herstel.

5. Digital Omnibus — mogelijk uitstel (niet op rekenen)

Op **19 november 2025** kwam het EU-voorstel **Digital Omnibus**.

- Daarin schuift de **hoog-risico-deadline mogelijk naar december 2027**.
- **Nog niet definitief** — niet op rekenen, geen zekerheid.
- Maar het geeft, als het doorgaat, **tijd voor een kleine, veilige fase 1**.

Openingszin voor de call

"Wij bouwen dit lokaal in Nederland, mens-in-de-lus, met DPIA en FRIA als bewijs — zodat jullie data nooit het land verlaat en jullie juridisch gedekt zijn. Dat is waarom dit bij ons veilig is en bij een cloud-partij niet."

Bronnen (geverifieerd)

Lokale / self-hosted modellen:

- GDPR Article 25 and Local AI: On-Premise LLM Inference Is Privacy by Design (Seresa)
- GDPR-Compliant AI: On-Premise & EU LLMs vs ChatGPT (ADVISORI)
- Self-Hosted LLM Guide: Run Llama & Mistral On-Prem (ZTABS)
- Running Local LLMs Privately: On-Prem AI Without Data Egress (Rapsols)

EU-cloud / data-residency:

- European Cloud Providers: GDPR-Compliant Hosting 2025 (DanubeData)
- GDPR-Approved AI Models for Europe (Almadetools)
- Microsoft completes EU Data Boundary (Microsoft On the Issues)

Juridisch — AVG / DPIA:

- DPIA — wanneer verplicht (Autoriteit Persoonsgegevens)
- Wanneer is een DPIA verplicht (ICTRecht)
- Regels voor AI & algoritmes (Autoriteit Persoonsgegevens)
- Verwerkersovereenkomst (Autoriteit Persoonsgegevens)
- Privacy by design & privacy by default (Ten Holter Noordam)
- Grondslagen AVG uitgelegd (Autoriteit Persoonsgegevens)

US-transfer / Schrems II:

- EU-US Data Privacy Framework survives first challenge (DLA Piper)
- EU-US data transfers (Europese Commissie)

EU AI Act / recruitment:

- EU AI Act en recruitment 2026-2027 (Recruitmenttraining)

- What the EU AI Act Means for Staffing Businesses (AI Act EU)