# MadEasy AI Browser – V2 Komplett Plan og Arkitektur

---

## 1) Mål og visjon

- **Automasjon på neste nivå:** Multi-agent orkestrering med spesialiserte roller.
- **Enterprise readiness:** sikkerhet, policyer, revisjon og flerbrukerstøtte.
- **Marketplace:** åpne for deling og installasjon av playbooks og plugins.
- **Mobil paritet:** Android med voice-first og raske workflows.
- **Kvalitet:** Preview-drevet QA som fanger feil tidlig, inkl. ytelse, a11y og visuell regresjon.

---

## 2) Epics

1. **Multi-agent orkestrering 2.0** – Planner, Critic, Executor, Researcher, Fixer.
2. **Watched Workflows & Scheduler** – repeterende playbooks, diff-deteksjon, varsler.
3. **QA Suite Pro** – Lighthouse-diff, axe-core, visuell regresjon, console error gates.
4. **Selector Studio + læringsprofiler** – stabilitets-score, fallback-læring pr. domene.
5. **Marketplace (Playbooks & Plugins)** – signerte pakker, vurderinger, sandbox-policy.
6. **Collaborative Mode** – delte sessions, kommentarer, review-regler.
7. **Security & Compliance+** – policy-simulator, redaksjon i logger, revisjonsspor.
8. **Android Paritet v2** – voice-first, hurtigplaybooks, Keystore/StrongBox Vault.
9. **MadEasy Voice v2** – hotword + push-to-talk, meeting mode med diarization, barge-in.
10. **Data & Observability v2** – KPI-dashboard, event-DAG, eksport til BI.

---

## 3) Arkitekturforsterkninger

- **Shared Core** via gRPC: orchestrator, qa, vision, voice, market.
- **Policy Guard**: evaluerer alle handlinger mot regler/scopes.
- **Task Graph**: avhengigheter, retries, kompensasjoner.
- **CAS-lagring**: content-addressable storage for skjermbilder/rapporter.
- **Telemetry**: strukturert logging + anonymisering.

### Arkitekturdiagram V2

MadEasy V2 Architecture

**Merk (compliance):** «Lead Data Vault» er admin-styrt og isolert fra sluttbrukere. Dersom dataene inneholder **personopplysninger** om personer i EU/EØS, vil **GDPR normalt fortsatt gjelde** for behandlingsansvarlig uavhengig av at sluttbrukere ikke kontrollerer lagringen. V2 leverer derfor **konfigurerbare «compliance modes»**: - *GDPR-kontrollert:* RLS, rettslig grunnlag (konfig), privacy-ledger, slett/innsyn, DPA/SCC dokumentasjon. - *Pseudonymisert/Hash:* sensitifiserte nøkler; opplåsing krever admin-prosess. - *Public-source only:* begrens til åpne kilder og felter uten privat karakter.

---

## 4) API-oppdateringer

- `qa_suite`: støtte for profiler og baseline-diff.
- `watch_workflow`: RRULE + triggers (content, element, status).
- `market.install` / `market.publish`: signering, manifest.
- `selector.stabilityScore(element)`: returnerer 0–100.
- `voice.start(mode, lang)`: streaming events.

---

## 5) Milepæler

- **M0 (uke 0–2):** Arkitektur, feature flags, migreringsplan.
- **M1 (uke 3–6):** Multi-agent 2.0, Selector Studio v2, QA Suite Pro del 1.
- **M2 (uke 7–10):** Watched Workflows, Marketplace (beta), Voice v2 grunnlag.
- **M3 (uke 11–14):** Collaborative Mode, Security+, Android paritet.
- **RC (uke 15–16):** Stabilisering, dokumentasjon, demo.

---

## 6) Sprintplan

**Sprint 1 (2 uker):** - Orchestrator v2 (task graph + policy hook). - Selector Studio v2 (stabilitets-score). - QA Suite Pro (LH-diff, console gate). - Voice v2 (hotword + PT-T). - KPI-instrumentering.

**Sprint 2 (2 uker):** - Watched Workflows (RRULE, diff). - Marketplace alpha (lokal installasjon + sandbox). - QA Suite Pro (visuell regresjon). - Collaborative grunnlag (read-only sessions).

---

## 7) KPIer

- **Automasjonsrate:** ≥70% playbooks uten manuell intervensjon.
- **Stabilitet:** ≥40% færre selector-feil.
- **Kvalitet:** ≥90% reduserte kritiske a11y-funn før merge.
- **Produktivitet:** 25–40% færre iterasjoner til grønn gate.
- **Engasjement:** ≥30 community-playbooks i Marketplace.

---

## 8) Risiko & mitigasjon

- **Anti-bot/ToS:** pacing, HIL-sjekkpunkter.
- **Ytelse:** lokal akselerasjon, batch, throttling.
- **Sikkerhet:** strenge scopes, release-once secrets, policy-simulator.
- **Android begrensning:** lite-profiler, tydelig støtte-matrise.

---

## 9) Multi-agent orkestrering 2.0 (detaljer)

**Roller:** Planner (plan), Critic (risiko/kvalitet), Executor (handling), Researcher (kildeinnhenting), Fixer (feilretting).

**Tilstandsmodell:** plan → propose → review → execute → validate → fix* → done/escalate.

**Meldingsskjema:** JSON med rolle, intent, proposal, asserts, evidence, decision.

**Consensus:** Planner+Critic kjører «short debate» (≤3 runder). Ved konflikt → human-in-the-loop.

---

## 10) Policy Guard (regelmotor)

**Formål:** Evaluere hver handling mot policyer (domene, risiko, bruker-scope).

**Regel-skjema:** YAML med scopes og policies. Simulator for dry-run.

---

## 11) Selector Studio v2

**Stabilitets-score (0–100):** basert på ARIA, synlig tekst, data-attributes, dom-dybde, sibling-varians.

**Profiler:** per domene med preferred selectors, fallbacks, anti-patterns.

---

## 12) QA Suite Pro (profiler & diff)

**Profiler:** definert i YAML. LH-min, axe-block-levels, routes, forms, visual regression baseline, console gates.

**Rapport:** LH diff, visuelle deltas, konsollfeil. Publiseres i PR.

---

## 13) Watched Workflows & Scheduler

**RRULE:** f.eks. ukentlig hver mandag 07:00. **Triggers:** content change, element change, status change. **Actions:** kjør playbook, opprett PR, send varsel.

---

## 14) Marketplace (Playbooks & Plugins)

**Manifest:** JSON med name, version, author, permissions, entry, signatur. **Policy:** sandbox krever samsvar mellom manifest og runtime. **Publishing:** signering → scanning → listet i katalog.

---

## 15) Collaborative Mode

- Live cursors, delte sessions, kommentarer med @mentions.
- Review-regler: 2 øyne på kritiske endringer.
- Sessions logges med events og deltagere.

---

## 16) Android Paritet v2

- Voice-first UI, Quick Playbooks.
- Vault koblet til Keystore/StrongBox.
- Lite QA: enkle sjekker lokalt, LH kjøres server-side.

---

## 17) MadEasy Voice v2

- STT: Whisper (DirectML Windows, lite Android).
- Hotword/PTT + barge-in.
- Diarization i møte-modus, oppsummering til arkiv.
- Events: partial_transcript, final_transcript, intent.

---

## 18) CI/CD maler

**GitHub Actions PR-gate:** kjør QA runner i pipeline. **Release pipeline:** bygg artefakter, signering (MSIX/electron), opplasting.

---

## 19) Telemetry & personvern

- Event DAG, sampling.
- Privacy ledger: retention, anonymisering.
- Eksport: CSV/Parquet for BI.

---

## 20) Migrering V1 → V2

- Kompatibilitetslag for playbooks.
- Policy Guard: starter som advarsel, går til blokk.
- QA profiler per domene.

---

## 21) Åpne spørsmål

- Betalte pakker i Marketplace V2 eller V2.1?
- Hvor strenge skal default policyer være?
- Minstestøtte for Android WebView features?

## 22) Lead Data Vault (admin-only, global, Non-EU default)

**Default (Non-EU drift):** Lead Vault kjører som en **admin-kontrollert database uten sluttbrukerrettigheter**. Alle leads (scrapet/samlet) lagres her i tillegg til at brukeren kan lagre/eksportere lokalt som vanlig. Vaulten fungerer dermed som et **sentralisert arkiv for admin** med enrichment, dedup og scoring. Brukere har aldri lesetilgang – kun admin via Read-Access Layer. GDPR-mekanismer er ikke aktivert som standard.

**Opsjonelle compliance-moduser:** - **GDPR-kontrollert:** for EU/EØS-marked, med RLS, privacy ledger, slett/innsyn, rettslig grunnlag. - **Pseudonymisert/Hash:** fingerprint-lagring; PII krever admin-prosess. - **Public-source only:** begrens til åpne kilder.

### 22.1 Arkitektur

Browser → Ingestion API (mTLS+signatur) → Enrichment → Dedup/Scoring → Lead Data Vault (Postgres RLS, Admin-only) → Read-Access Layer (eksport) → Audit/Compliance.

### 22.2 Datamodell

- **lead** (id, fingerprint, source_url, collected_at, collector_id, raw_blob, normaliserte felter)
- **enrichment** (lead_id, provider, payload, confidence)
- **score** (lead_id, fit, reach, intent, credibility, total)
- **audit_log** (event_id, actor, action, hash_prev, hash_curr)

### 22.3 Dedup & scoring

Fingerprint + fuzzy-match; merge policy; retention (konfigurerbar TTL).

### 22.4 Tilgang & policy

- RLS: kun admin leser, ingestor kan kun insert.
- Policy Guard: blokkerer alle klient-reads.
- Eksport via Admin-lag, ikke direkte DB.

### 22.5 Enrichment

Verifisering (MX/SMTP, HLR), firmografi, geo, normalisering, prioritering.

### 22.6 Sikkerhet

mTLS+signatur på ingest, PII-maskering i logger, audit hash-kjede.

### 22.7 Integrasjon

Playbooks sender alltid via ingest-step.

### 22.8 Admin-verktøy

Søk/filtrer, merge, manuell enrichment, eksport til CRM.

## 22.9 Overvåkning

Contract tests, dedup-rapporter, alarmer på ingest/RLS-brudd.

## 22.10 Sekvens: Dobbel lagring (lokalt + Vault)

Dual Storage Sequence

**Forklaring:** Når en playbook kjører, eksporterer browseren data **lokalt** (CSV/XLSX/JSON) for brukeren *og* sender samtidig et normalisert, signert payload via **Ingestion API** (mTLS) til Lead-tjenestene for enrichment/dedup/scoring før lagring i **Lead Data Vault (Admin-only, RLS)**.