VCA-tool: hoe bewaar je de persoonsgegevens AVG-proof?

Dit advies bouwt voort op de AVG-research die we op 29 juni deden voor het GreenFox/Greenvox-project (AVG-proof lokale AI, geen US-cloud) en past die toe op Erik's VCA-vraag. Het is samengesteld door Conductor sámen met Hermes (tweede blik op de architectuur). **Belangrijk vooraf: dit is praktisch advies, geen juridisch bindend oordeel — laat een FG of privacy-jurist de definitieve opzet toetsen.**

Het probleem in het kort

De VCA-administratie bestaat uit twee "hopen":

1. **Algemene hoop** — formulieren, regelgeving, ondertekeningen, naleving. Weinig privacy-gevoelig.
2. **Persoonsgegevens-hoop** — interviews, ingevulde formulieren met **paspoortgegevens, telefoon, e-mail en IBAN-nummers**. Zeer gevoelig, moet AVG-proof beschermd.

Erik's idee: zet die tweede hoop op een **aparte lokale schijf** die normaal NIET gekoppeld is, en koppel 'm alleen tijdelijk aan de laptop tijdens een interne/externe audit. Dat idee is goed — hieronder hoe je het waterdicht maakt.

Het advies: gescheiden + versleuteld + minimaal gekoppeld

1. De aparte versleutelde schijf — JA, verstandig

Een schijf die normaal losgekoppeld is (bijna "air-gapped") verkleint het risico enorm. Doe het zo:
- **Volledige schijfversleuteling, minimaal AES-256.** Gratis + degelijk: **VeraCrypt** (open-source). Of BitLocker (Windows) / FileVault-container (Mac).
- Zonder ontgrendeling is de data fysiek onleesbaar — óók als de laptop of schijf gestolen wordt.
- De persoonsgegevens staan **volledig los** van het algemene systeem.

2. Sleutelbeheer — dit is het meest kritieke punt

- Bewaar het wachtwoord/de sleutel **NOOIT op dezelfde laptop**.
- Gebruik bij voorkeur een **hardware-token (YubiKey)** of bewaar de herstelsleutel offline (papier in een kluis).
- **Twee-factor voor ontgrendeling** (wachtwoord + fysieke token) is het minimum voor gegevens van dit niveau.

3. Het invulproces — direct naar het beschermde deel

- Als een medewerker een formulier invult, moet dat **direct** in de versleutelde container geschreven worden.
- **Geen tussentijdse temp-bestanden** op de gewone (onbeveiligde) laptop-schijf — dat is een klassiek lek.

4. Audit-toegang veilig regelen

- Koppel de schijf alleen bij een audit, **onder het vier-ogen-principe** (twee medewerkers erbij).
- **Log elke koppeling**: datum, tijd, wie, waarvoor. Na de audit: ontkoppelen + logboek bijwerken.
- Externe auditor: geef **minimale inzage** — overweeg een tijdelijk, gefilterd exportbestand met alleen wat ze nodig hebben, i.p.v. volledige schijftoegang.

5. Backup — vergeet dit niet

- Een versleutelde schijf die kapotgaat = alles kwijt. Maak een **versleutelde off-site backup** (bv. een eigen NAS met encryptie, of een end-to-end versleutelde dienst zoals Tresorit).
- **Nooit** naar een standaard clouddienst zonder end-to-end encryptie (en geen Amerikaanse cloud — sluit aan op de GreenFox-lijn: data blijft in eigen beheer/EU).

De AVG-kant (waar je op moet letten)

- **Paspoortgegevens** zijn identiteitsbewijs-data (Wid art. 8) — je hebt een **expliciete grondslag** nodig (wettelijke verplichting of uitdrukkelijke toestemming) en mag ze na verificatie vaak niet lang bewaren.

- **IBAN** = gewone persoonsgegevens, maar financieel gevoelig.
- **Verwerkingsregister** aanleggen (verplicht bij >250 medewerkers, maar ook voor het MKB sterk aanbevolen): per gegeven → doel, grondslag, bewaartermijn, wie toegang heeft.
- **Dataminimalisatie** (AVG art. 5): sla alleen op wat écht nodig is voor de VCA-administratie. Niet meer.
- **Bewaartermijnen + jaarlijkse opschoning**: leg vast hoe lang je wat bewaart en ruim de rest gestructureerd op. ID-bewijs zo snel mogelijk na verificatie vernietigen.
- **DPIA-drempel**: bij systematische verwerking van ID-bewijs + financiële gegevens van medewerkers in een nieuw systeem is er een serieuze kans dat een **DPIA (art. 35 AVG) verplicht** is. Check dit met de AP-DPIA-tool of via een FG — niet doen = risico bij een incident.
- **Meldplicht bij diefstal/verlies**: is de data aantoonbaar goed versleuteld (met sleutel elders bewaard), dan val je bij verlies van de laptop meestal **buiten** de 72-uurs meldplicht. Dat is precies waarom de encryptie + apart sleutelbeheer zo belangrijk is — documenteer dit.

Valkuilen (kort)

- Backup van de versleutelde schijf vergeten → bij schijfuitval alles kwijt.
- Temp-bestanden op de onbeveiligde schijf tijdens invullen → lek.
- Toegangsrechten niet vastgelegd → bij vertrek medewerker meteen sleutel/wachtwoord roteren.

Concrete volgende stappen

1. **Technisch (kan Conductor/Sjakie bouwen/inrichten):** VeraCrypt-container op een aparte schijf, invulformulieren die direct naar die container schrijven, koppel-logboek, versleutelde off-site backup.
2. **Juridisch (mens/FG):** laat een FG of privacy-jurist de **DPIA-noodzaak** beoordelen, het **verwerkingsregister** opstellen en de grondslagen + bewaartermijnen vastleggen. De techniek hierboven is solide voor een klein bedrijf, maar de juridische borging vereist professionele toetsing.

In één zin

Erik's aanpak (aparte, alleen-bij-audit-gekoppelde schijf) is goed — maak 'm waterdicht met **sterke versleuteling + sleutel apart bewaard + direct-naar-container-invullen + gelogde audit-toegang + versleutelde backup**, en laat de juridische kant (DPIA + register) door een FG toetsen.

Advies door Conductor + Hermes, 8 juli 2026. Bouwt voort op de GreenFox/Greenvox AVG-research (29 juni). Geen juridisch bindend oordeel — laat een FG/privacy-jurist de opzet formeel toetsen.