

VCA-startpakket

Voor Jamal en Erik. Dit is de uitvoering van stap 0 en stap 1 uit het topplan (<https://verslag.haartips.nl/r-vca-topplan.html>). Drie onderdelen: de privacy-aanzet voor de jurist, de vragen die Erik moet beantwoorden, en de reparatielijst voor het dossier. Alles direct bruikbaar.

Onderdeel 1 – DPIA-aanzet (voor de FG of privacy-jurist)

Dit is de voorbereiding die de jurist nodig heeft om de verplichte DPIA te toetsen.

De AP zegt: start in de ontwerpfase — dat is nu.

Wat het systeem gaat verwerken:

CATEGORIE	VOORBEELDEN	GRONDSLAG	BEWAARTERMIJN
Personeelsdossier vast	naam, adres, ID-kopie, BSN, salaris	wettelijke plicht (Wet loonbelasting art. 28)	ID-kopie 5 jaar, salaris 7 jaar, rest 2 jaar na uitdienst
Inleners (EER)	naam, geboortedatum, BSN, ID-nummer — GEEN kopie	ketenaansprakelijkheid	registratieplicht-termijnen
ZZP'ers	naam, contact, tarief, contract — GEEN ID-kopie	uitvoering overeenkomst	fiscale termijnen
Veiligheidsregistraties	toolbox-presentie, aftekeningen, inspecties, incidenten	gerechtvaardigd belang + norm-/zorgplicht	minimaal 3 jaar (VCA-eis)
Certificaten/diploma's	B-VCA, VOL-VCA, aanwijzingen NEN 3140	normplicht (mustvragen 3.2/3.3)	duur dienstverband + certificaatcyclus

Wat het systeem NOOIT verwerkt: medische gegevens (horen bij de arbodienst), strafrechtelijke gegevens, afkomst. VOG's worden niet bewaard, alleen "gezien op datum".

Waarom een DPIA verplicht is: werknemers gelden bij de AP als kwetsbare groep, en het systeem monitort activiteiten (aftekeningen, aanwezigheid) op schaal — dat raakt minstens 2 EDPB-criteria plus de AP-categorie "monitoring werknemers".

De maatregelen die al ontworpen/uitgevoerd zijn:

1. Persoonsgegevens gescheiden van de systeemkant (Erik's twee-hopen-model, 8-7)
2. AES-256-versleutelde opslag, sleutel apart van de data (uitgevoerd 2-8)
3. Dataminimalisatie per contractvorm hard afgedwongen (geen ID-veld voor ZZP'ers)
4. Audit-toegang gelogd, vier-ogen-principe
5. Hosting in Nederland, geen Amerikaanse cloud
6. Volledige aftekening-audit-trail (wie, wat, wanneer)

Vraag aan de jurist: DPIA toetsen + verwerkingsregister + verwerkersovereenkomst-sjabloon (voor als andere bedrijven klant worden). Alles hierboven is voorwerk, geen juridisch oordeel.

Onderdeel 2 — De vragen die Erik moet beantwoorden (staan open sinds 23 juni)

1. **Rollen en personen.** Wie zijn de IV, WV's, VP's en VOP's (NEN 3140-aanwijzingen)?
Wie levert wat aan (toolbox leiden, inspecties lopen, keuringen doen)? Met contactgegevens per persoon.
2. **Kanaal per persoon.** Hoe wil ieder zijn herinneringen krijgen: WhatsApp, mail of web-app? (Erik zei 17-6: "iedereen heeft een telefoonnummer" — WhatsApp ligt voor de hand, maar het moet per persoon vastliggen.)
3. **Waar draait het.** Eigen beveiligde web-app (de voorkeur uit het 17-6-gesprek), of koppelen aan iets bestaands?
4. **NIEUW, uit de kruiscontrole: wat is Michelle's formele rol?** Er ligt een HVK-diploma in het dossier. De norm eist een VGM-functionaris op MVK-niveau die rechtstreeks aan de directie rapporteert — een HVK'er voldoet ruimschoots. Als

Michelle die rol formeel krijgt (organogram + functieomschrijving), is mustvraag 1.2 in één keer sterk gedekt.

Onderdeel 3 – Reparatielijst dossier (direct auditwaarde, vóór er software is)

Erik wordt bij de volgende controle (~zomer 2027) getoetst tegen norm 2026/6.1, VCA** = 28 mustvragen. Dit zijn de gaten, op volgorde van normrisico:

#	REPARATIE	NORMVRAAG	NU
1	Meldingen-register 2024/2025 rechtekken: waren er echt nul incidenten of is er niet geregistreerd? Vastleggen wat waar is	11.1 + 11.2 (must)	2 jaar leeg
2	RI&E actualiseren voor 2026	2.1 (must) + Arbowet art. 5	niets in 2026
3	VGM-bewustzijnsprogramma aandikken — voor VCA** verplicht	4.2 (must voor **)	2-3 stukken/jaar
4	Actuele registratie personeel-certificaten opbouwen (B-VCA/VOL-VCA per persoon met vervaldatum)	3.2 + 3.3 (must)	alleen archief
5	Teamoverleg herstarten met agenda + presentielijst	4.1- ondersteunend	2,5 jaar stil
6	Werkplekinspectie juli 2026 inhalen + vastleggen dat de directie 1x per kwartaal meeloopt	7.1 (must)	juli mist; kwartaal-deelname niet aantoonbaar
7	Toolbox-presentie: volledige namen + handtekeningen controleren (norm eist geen initialen)	4.1 (must)	inspecteurs werken met initialen

#	REPARATIE	NORMVRAAG	NU
8	Formulierenstelsel opschonen: het dubbele nummer 031, P&O-014 in History, spelling P&O-/PO-	voorwerk digitalisering	nummerconflicten
9	Dossier omhangen naar 6.1-structuur (incl. nieuwe mustvraag 1.7: wetgevings-systematiek — tot de tool live is: een simpele kwartaal-check met bronnenlijst)	1.7 (nieuw, must)	bestaat niet

Punt 1 t/m 6 is werk voor Erik (met deze lijst in de hand). Punt 7 t/m 9 kan ik voorbereiden zodra het bouwen start.

Wat hierna komt

Zodra Erik de vragen uit onderdeel 2 beantwoordt, bouw ik fase 2 uit het plan van 23 juni: de digitale formulieren-demo langs zijn eigen P&O-stelsel — de klus-start-flow, de inspectie-flow en de toolbox-registratie met teller en handtekeningen. Dat is meteen de klikbare demo voor het grotere SaaS-verhaal.

Verzending naar Erik: pas na Jamals akkoord.