

VERDIEPINGSDOCUMENT

Compliance by design

Hoe door AI gegenereerde PRINCE2® 7-projectdocumentatie aansluit op NIS2, de Baseline Informatiebeveiliging Overheid 2, de Algemene verordening gegevensbescherming, ISO 31000 en opkomende AI-regelgeving, zonder dat de AI ooit namens u claimt dat aan de regels is voldaan.

DOCUMENTTITEL	Compliance by design: door AI gegenereerde PRINCE2® 7-documentatie voor de publieke sector
TYPE	Verdiepingsdocument
DOEL	Toelichten hoe Besluitklaar.AI door AI gegenereerde projectdocumentatie afstemt op PRINCE2 7, NIS2, de Baseline Informatiebeveiliging Overheid 2, de Algemene verordening gegevensbescherming en internationale normen
STATUS	Vastgesteld door de productowner
VERSIE	1.0
DATUM	10 oktober 2026
AUTEUR	Productteam Besluitklaar.AI
EIGENAAR	Harco Bouwman, productowner Besluitklaar.AI
CLASSIFICATIE	Openbaar
REIKWIJDTE	Publieke organisaties in Nederland en de Europese Unie; partners en licentiegevers

MANAGEMENTSAMENVATTING

Snelheid zonder concessies aan verantwoording

IT-projecten in de publieke sector werken binnen een groeiend aantal verplichtingen. Eén Project Brief moet consistent zijn met PRINCE2 7, de eisen voor informatiebeveiliging uit de Baseline Informatiebeveiliging Overheid 2 en NIS2 weerspiegelen, de privacyverplichtingen uit de Algemene verordening gegevensbescherming herkennen en steeds vaker rekening houden met de EU AI-verordening. Projectmanagers besteden een onevenredig deel van hun tijd aan het vertalen van deze kaders naar documentatie, terwijl stuurgroepen documenten nodig hebben die zij kunnen vertrouwen wanneer zij een besluit nemen.

Generatieve AI kan die cyclus sterk verkorten. Tegelijk brengt zij een nieuw risico met zich mee: een model dat gaten opvult met aannemelijke inhoud, of dat een oordeel over compliance presenteert dat het niet mag geven. In de publieke sector is dat geen kwaliteitsprobleem. Het is een governanceprobleem.

Besluitklaar.AI is ontworpen rond één principe dat deze spanning oplost: de agent signaleert, mensen bepalen. Elke output is gebaseerd op de aangeleverde input, elke uitspraak is herleidbaar, elk gat wordt gemarkeerd in plaats van opgevuld, en elk compliance-aandachtspunt wordt doorgezet naar de rol die ervoor verantwoordelijk is.

KERNPUNTEN

- 1 Compliance is ingebouwd, niet achteraf toegevoegd.** PRINCE2 7, de Baseline Informatiebeveiliging Overheid 2, NIS2 en de Algemene verordening gegevensbescherming zijn verankerd in de systeemprompt, de kennisbronnen en de vaste outputstructuur van elke agent.
- 2 De agent claimt nooit compliance.** Hij benoemt aandachtspunten en verwijst die naar de informatiebeveiligingsfunctionaris, de functionaris gegevensbescherming of de risico-eigenaar. De classificatie van informatie laat hij altijd aan de organisatie.
- 3 Onzekerheid wordt expliciet gemaakt.** Voordat de agent een concept opstelt, beoordeelt hij de kwaliteit van de input. Ontbrekende informatie wordt als zodanig gemarkeerd en nooit vervangen door aannemelijke inhoud.
- 4 De mens houdt de regie.** Output van de agent is altijd een concept (versie 0.x). Alleen de projectmanager kan het vaststellen als versie 1.0.

SECTIE 1

De compliance-uitdaging in publieke projecten

Projectdocumentatie bij de overheid is meer dan administratie. Een Project Brief of Project Initiation Documentation is de basis waarop een stuurgroep publieke middelen vastlegt, risico's accepteert en verantwoordelijkheden toewijst. De documentatie moet daarom twee publieken tegelijk bedienen: de projectmethode en het wettelijke en regelgevende kader waarbinnen de organisatie werkt.

Vier krachten die samenkomen

- **Dichtheid van regelgeving.** NIS2, de Baseline Informatiebeveiliging Overheid 2, de Algemene verordening gegevensbescherming en de EU AI-verordening brengen elk verplichtingen met zich mee die vroeg in een project herkend moeten worden, niet pas bij de livegang.
- **Consistente methode.** PRINCE2 7 verwacht dat managementproducten volledig zijn, op maat gemaakt en consistent met de zeven performance targets, inclusief duurzaamheid.
- **Beperkte capaciteit.** Ervaren projectmanagers zijn schaars, en documentatie concurreert met uitvoering om hun tijd.
- **Vertrouwen in AI-output.** Besluitvormers moeten weten welke uitspraken feiten uit de bron zijn, welke aannames zijn en welke informatie nog ontbreekt.

Waarom generieke AI-hulpmiddelen tekortschieten

Algemene assistenten zijn geoptimaliseerd voor vloeiende, volledig ogende antwoorden. In projectgovernance is dat precies het faalpatroon dat u wilt vermijden: een stellige alinea over budget, scope of informatieclassificatie zonder basis in het mandaat kan een stuurgroep tot een besluit op onjuiste gronden brengen. Besluitklaar.AI kiest bewust het tegenovergestelde: een onvolledig maar eerlijk concept is waardevoller dan een volledig maar ongefundeerd document.

SECTIE 2

Onze positie: signaleren, nooit bepalen

Elk kader maakt onderscheid tussen het herkennen van een verplichting en het oordeel of eraan is voldaan. De agents van Besluitklaar.AI werken uitsluitend aan de eerste kant van die lijn. Deze scheiding is vastgelegd in de agent-ontwerpstandaard en in elke systeemprompt.

Onderwerp	Wat de agent doet	Wat de agent nooit doet
Informatiebeveiliging	Signaleert beveiligingseisen, risico's en maatregelen in de relevante onderdelen	Een informatieclassificatie toekennen. Die wordt altijd gemarkeerd als "Door de informatiebeveiligingsfunctionaris of functionaris gegevensbescherming vast te stellen"
Zorgplicht NIS2	Signaleert zorgplicht en meldplicht voor incidenten in de onderdelen over risico's en governance	Bepalen of de organisatie onder NIS2 valt
Persoonsgegevens	Signaleert verwerking van persoonsgegevens en stelt de vraag of een effectbeoordeling voor gegevensbescherming nodig is	De vraag naar een effectbeoordeling voor gegevensbescherming beantwoorden of de rechtmatigheid beoordelen
Risico	Stelt kandidaat-risico's voor met een gestructureerde risicotaxonomie; kans en impact blijven open voor beoordeling door de risicomanager	Kans of impact vaststellen, of een risico accepteren, afwijzen of in eigendom nemen
Vaststelling	Levert een te beoordelen concept met expliciete gaten en vragen	Een document goedkeuren of verheffen tot versie 1.0

SECTIE 3

Afstemming op kaders

De tabel hieronder vat samen hoe elk kader wordt toegepast. "Ingebouwd" betekent dat het kader de structuur en het gedrag van de agent bepaalt. "Gesignaleerd" betekent dat de agent relevante verplichtingen benoemt voor beoordeling door mensen. "Referentie" betekent dat het kader richting geeft aan ons ontwerp en beheer, zonder claim van certificering of conformiteit.

Kader	Reikwijdte	Hoe Besluitklaar.AI het toepast	Rol
PRINCE2® 7	Projectmanagementmethode: principes, practices, processen, managementproducten en zeven performance targets	Vaste productstructuren voor de Project Brief en de Project Initiation Documentation; consistente PRINCE2-terminologie; toleranties voor alle zeven performance targets, inclusief duurzaamheid	INGEBOUWD
Baseline Informatiebeveiliging Overheid 2	Baseline voor informatiebeveiliging van de Nederlandse overheid: risicogebaseerd, met een verplicht managementsysteem op basis van ISO/IEC 27001 en 27002:2022	Beveiligingseisen en maatregelen per onderdeel gesignaleerd; geen gebruik van de vervallen basisbeveiligingsniveaus; classificatie gelaten aan de organisatie	GESIGNALEERD
NIS2	Europese richtlijn 2022/2555 voor netwerk- en informatiebeveiliging, in Nederland uitgewerkt in de Cyberbeveiligingswet	Zorgplicht en meldplichten gesignaleerd in de onderdelen over risico's en governance; bepaling van de reikwijdte gelaten aan de organisatie	GESIGNALEERD
Algemene verordening gegevensbescherming	Europese verordening 2016/679, met privacy by design (artikel 25) en effectbeoordelingen voor gegevensbescherming (artikel 35)	Verwerking van persoonsgegevens en de noodzaak van een effectbeoordeling gesignaleerd; dataminimalisatie toegepast op de inhoud die de agent maakt	GESIGNALEERD
ISO 31000:2018	Internationale richtlijn voor risicomanagement: identificatie, analyse, evaluatie en behandeling	De Risk Agent werkt met een gestructureerde risicotaxonomie en een vaste regelset; kans en impact worden beoordeeld en vastgesteld door de risicomanager	INGEBOUWD
ISO/IEC 27001:2022	Internationale norm voor managementsystemen voor informatiebeveiliging	Indirect toegepast via de Baseline Informatiebeveiliging Overheid 2; de agent verwijst naar beheersmaatregelen zonder de invoering ervan te beoordelen	REFERENTIE
EU AI-verordening	Verordening (EU) 2024/1689 over artificiële intelligentie: transparantie en menselijk toezicht	Ontwerp als beslisondersteuning met menselijk toezicht bij elke stap, transparante markering van door AI gemaakte inhoud en volledige herleidbaarheid	REFERENTIE
ISO/IEC 42001:2023	Internationale norm voor managementsystemen voor artificiële intelligentie	Richt het beheer van de levenscyclus van de agents in: ontwerpstandaard, versiebeheer, testen en gecontroleerde vrijgave	REFERENTIE

SECTIE 4

Hoe compliance by design in de praktijk werkt

Stap 1: de agent beoordeelt eerst de input

Voordat de agent inhoud genereert, beoordeelt hij de kwaliteit van het startdocument, zoals een projectmandaat. Hij controleert of de kernelementen voor een besluit aanwezig zijn: achtergrond, probleemstelling, gewenste verandering, opdrachtgever, scope en uitsluitingen, kaders voor tijd en budget, belanghebbenden, en risico's, aannames en afhankelijkheden. Het resultaat is een van drie beoordelingen, die samen met de ontbrekende elementen aan de projectmanager wordt gemeld.

Beoordeling	Gevolg voor het concept
Voldoende	Concept geschikt voor beoordeling door de projectmanager
Beperkt	Concept gemarkeerd als "Niet geschikt voor besluitvorming"; ontbrekende elementen opgesomd met gerichte vragen
Onvoldoende	Concept gemarkeerd als "Niet geschikt voor besluitvorming"; alleen informatie over de kernelementen wordt als feit vastgelegd

Stap 2: elke uitspraak krijgt een markering

In het document krijgt elke inhoudelijke uitspraak een van vier vaste markeringen. Zo zien beoordelaars en besluitvormers in één oogopslag hoe betrouwbaar de inhoud is.

Markering	Betekenis
Feit	Rechtstreeks overgenomen uit de input, met bronvermelding
Aanname	Een redelijk werkuitgangspunt dat geverifieerd moet worden
Nog aan te vullen	Ontbrekende informatie, met één gerichte vraag aan de projectmanager
Aandachtspunt	Een overweging, vaak op het gebied van regelgeving, die menselijke validatie vraagt door de verantwoordelijke rol

Stap 3: een vaste, auditbare output

Elke output volgt de hoofdstukindeling van het geldende sjabloon, dat voorgaat op de prompt wanneer die verschillen. Een metadatablok van veertien velden bovenaan legt het documenttype, de agent en versie, de fase in de levenscyclus, de bronnen, de classificatiestatus, de beoordelingsverantwoordelijkheid en de inputbeoordeling vast, zodat de herkomst van elk document achteraf te reconstrueren is.

Stap 4: de mens valideert

Output van de agent is altijd versie 0.x, een concept ter beoordeling. De projectmanager beoordeelt, vult aan en corrigeert het, en is de enige die het kan verheffen tot versie 1.0. De stuurgroep besluit vervolgens op basis van een gevalideerd document, niet op basis van AI-output.

SECTIE 5

Negen ontwerpprincipes

Alle agents van Besluitklaar.AI worden gebouwd en beoordeeld aan de hand van dezelfde negen principes. Ze gelden als acceptatiecriteria voor elke nieuwe agent voordat die in productie gaat.

#	Principe	Betekenis
P1	Geground	Inhoud is uitsluitend gebaseerd op de aangeleverde input en goedgekeurde kennisbronnen; geen verzonnen feiten, cijfers of wetsbepalingen
P2	Herleidbaar	Elke inhoudelijke uitspraak is te herleiden tot een bron, een inputveld of een expliciete aanname
P3	Mens in de lus	Output is een te beoordelen concept, nooit een besluit; punten die menselijk oordeel vragen, worden gemarkeerd
P4	Conform PRINCE2 7	Structuur, terminologie en producten volgen PRINCE2 7
P5	Compliance by design	De Baseline Informatiebeveiliging Overheid 2, NIS2 en de Algemene verordening gegevensbescherming zijn verankerd in de prompt en het outputcontract
P6	Deterministische structuur	De vorm van de output ligt vast; alleen de inhoud verschilt per project
P7	Expliciete onzekerheid	Ontbrekende of tegenstrijdige input leidt tot gemarkeerde gaten, niet tot verzonnen inhoud
P8	Scheiding van verantwoordelijkheden	Eén agent, één duidelijk afgebakend managementproduct, verbonden via vastgelegde input- en outputcontracten
P9	Auditbaar	Metadata, versies en besluiten worden vastgelegd, zodat elk document te reconstrueren is

SECTIE 6

Platform, gegevenslocatie en vrijgavebeheer

Besluitklaar.AI draait op Microsoft Copilot Studio en het Microsoft Power Platform, de omgeving die veel Nederlandse overheidsorganisaties al gebruiken. De inrichting is zo ontworpen dat het beheer van het hulpmiddel de governance weerspiegelt die het ondersteunt.

Gegevenslocatie en toegang

- **Europese hosting.** De productieomgeving draait in de Microsoft-regio Zwitserland, binnen de reikwijdte van de EU Data Boundary van Microsoft.
- **Beheerste toegang.** Toegang is beperkt tot een vaste beveiligingsgroep. Gebruikers loggen in met hun eigen organisatieaccount en meervoudige verificatie via Microsoft Entra ID.
- **Gescheiden omgevingen.** Ontwikkeling en productie draaien in aparte omgevingen, elk met een eigen beveiligings- en factureringsinrichting.

Vrijgavebeheer

- **Vrijgave in één richting.** Wijzigingen worden alleen in de ontwikkelomgeving gemaakt, als genummerde beheerde oplossing geëxporteerd en naar productie gebracht. Productie wordt nooit rechtstreeks aangepast.
- **Systeemprompts onder versiebeheer.** Elke systeemprompt valt onder versiebeheer en is gekoppeld aan de versie van de oplossing waarin hij wordt vrijgegeven.
- **Testen vóór vrijgave.** Elke agent heeft een testset, met single-turn-gedrag als eerste testcategorie, voordat hij live gaat.

WAT DIT BETEKENT VOOR UW ORGANISATIE

Uw informatiebeveiligingsfunctionaris, functionaris gegevensbescherming en risicomanager blijven de beslissers bij elke compliancevraag. Besluitklaar.AI zorgt dat die vragen hen vroeg, consistent en met een helder controlespoor bereiken, op het moment dat het project vorm krijgt in plaats van vlak voor de livegang.

SECTIE 7

Routekaart

De huidige versie omvat de Project Brief en de Project Initiation Documentation, ondersteund door een agent voor het risicoregister. Dezelfde ontwerpstandaard wordt toegepast op elk volgend managementproduct.

- **Extra managementproducten:** Business Case, Management Approaches, registers en voortgangsrapportages zoals het Highlight Report.
- **Opgemaakte documenten:** output als opgemaakt document met het metadatablok, klaar voor het projectarchief.
- **Meertalige output:** ondersteuning van andere talen dan het Nederlands voor internationale en grensoverschrijdende organisaties.

OVER BESLUITKLAAR.AI

Besluitklaar.AI ontwikkelt gespecialiseerde AI-agents die IT-projectmanagers bij publieke organisaties helpen consistente, toetsbare en besluitklare PRINCE2 7-documentatie op te stellen, met governance, risico en compliance ingebouwd.

Harco Bouwman, oprichter en productowner

Disclaimer. Dit verdiepingsdocument beschrijft de ontwerpintentie van Besluitklaar.AI. Het vormt geen juridisch advies, en Besluitklaar.AI certificeert of beoordeelt geen naleving van wet- en regelgeving of normen. De verantwoordelijkheid voor compliance blijft bij de organisatie en haar verantwoordelijke functionarissen.

PRINCE2® en PRINCE2 7® zijn geregistreerde handelsmerken van de PeopleCert-groep. Microsoft, Copilot Studio, Power Platform en Entra zijn handelsmerken van de Microsoft-groep. ISO- en IEC-normen worden aangeduid met hun gepubliceerde titels.