provincie Zuid-Holland

Herziene aanpak Programma Privacy

Afhandelen datalek en verhogen privacyvolwassenheid

12 sept 2024

Versie 1.5

Inhoudsopgave programmaplan Privacy

Reactie FG op programmaplan

Lijn 1:

Lijn 2:

Inleiding

Voor u ligt het vernieuwde programmaplan voor de aanpak van het datalek in iDMS en het verhogen van de privacy-volwassenheid binnen de provincie Zuid-Holland.

Eerdere plannen stuitten op enkele beperkingen tijdens de uitvoering. Daarbij is geïntensiveerd op tooling en het betrekken van data- en proceseigenaren om effectiever persoonsgegevens te kunnen identificeren. De nieuwe aanpak is beschreven in dit programmaplan.

In de afgelopen twee jaar heeft de provincie Zuid-Holland flink geïnvesteerd in het versterken van de privacy-organisatie en -uitvoering. Dit was nodig, omdat er tussen 2018 en 2022 te weinig vooruitgang werd geboekt op het gebied van privacy-volwassenheid. Uit een onderzoek van de Eenheid Audit en Advies in 2022 bleek dat de provincie slechts niveau 1 had bereikt op de volwassenheidsmatrix van het CIP, op een schaal van 1 tot 5. De directie heeft de ambitie uitgesproken om uiterlijk op 31 december 2026 niveau 3 te halen.

De urgentie van dit programma is verder toegenomen door een groot datalek in september 2023, wat aantoonde dat onze informatiebeheer niet voldoende op orde is. Hierdoor staat de provincie nu onder verscherpt toezicht van de Autoriteit Persoonsgegevens. Dit programma is gestart om zowel het datalek op te lossen als de privacy-volwassenheid van de organisatie te verbeteren. De concerndirectie heeft dit tot een topprioriteit gemaakt.

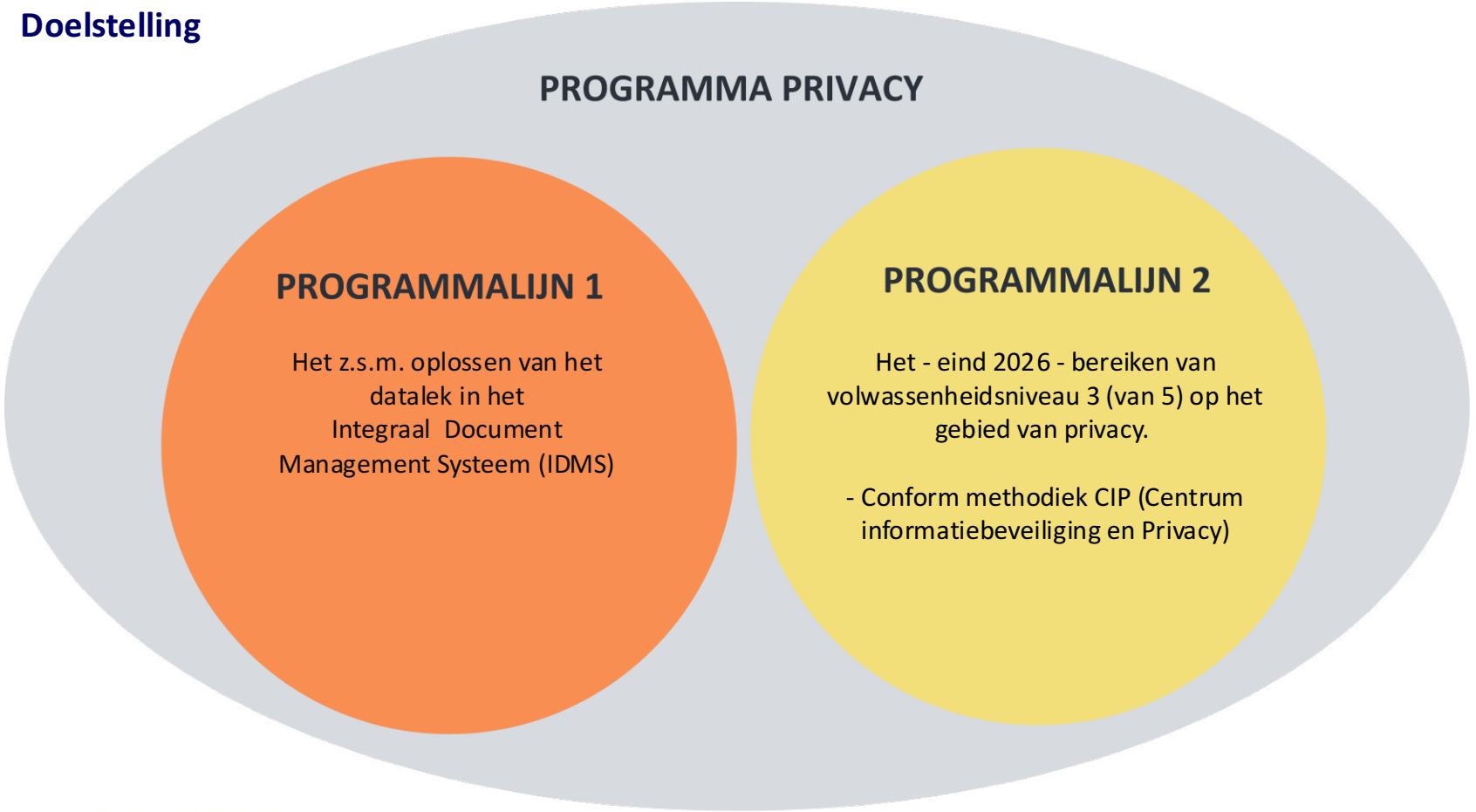
Relaties met andere opdrachten

Het oplossen van het datalek en de gewenste groei van de privacyvolwassenheid kan niet in een isolement plaatsvinden. Wat de organisatie als geheel heeft veroorzaakt, zal de gehele organisatie ook samen moeten oplossen. Daartoe is communicatie en activatie van medewerkers en management noodzakelijk.

Met lopende programma's en opdrachten wordt telkens onderzocht of reeds geplande of nieuwe activiteiten versneld kunnen worden uitgevoerd om privacydoelstellingen te bereiken.

- **Informatietransitie** speelt een belangrijke rol in het helpen dichten van het datalek. Het heeft verder als doel het informatiebeheer van de provincie Zuid-Holland te verbeteren. Het programma verhoogt de betrouwbaarheid van onze systemen en zorgt dat we informatie op een veilige en efficiënte manier kunnen beheren.
- **Informatieveiligheid** ontfermt zich over de beveiliging van (onder meer) persoonsgegevens;
- **De bewustwordingscampagne 'ZO Doen we Dat'** speelt een belangrijke rol om medewerkers te betrekken bij de informatiehuishouding;
- Het project **Learning Management Systeem (LMS)** is het platform waarmee de privacy-bewust-wordings-trainingen kunnen worden gegeven.
- Het project **Identity Access Management (IAM)** heeft als doel een geautomatiseerd systeem op te zetten voor het toekennen en intrekken van rechten op basis van rollen.

Doelstelling



Projectsturing

1. Uitvoering vindt plaats binnen het domein Bedrijfsvoering onder regie van de eenheid Privacy, maar het programma is niet ‘van’ de eenheid Privacy. Iedere medewerker heeft belang bij een veilige werkomgeving met privacy-gevoelige data en informatie

2. Inhoudelijke en implementatiekeuzes worden voorgelegd aan het kernteam en/of de stuurgroep.

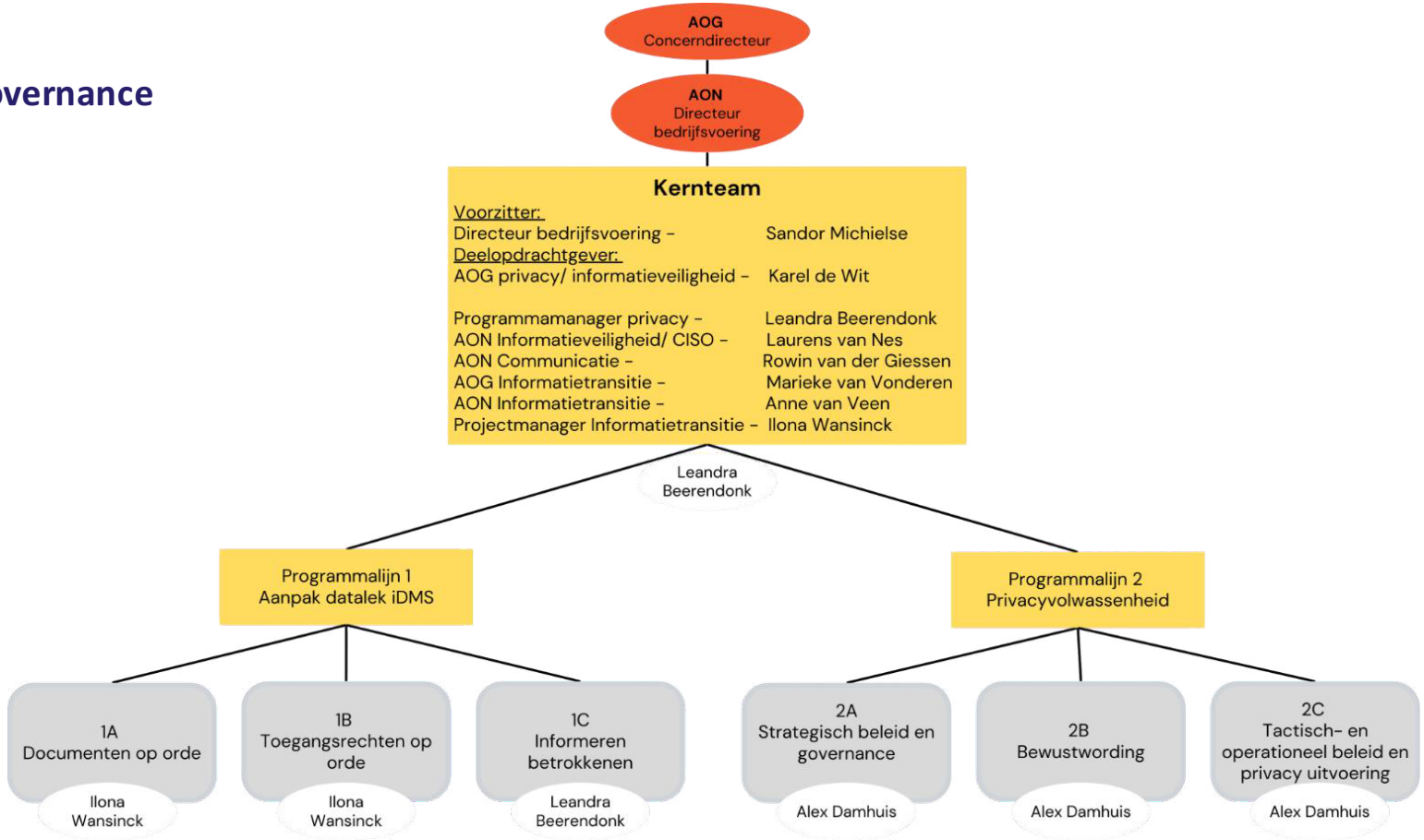
3. De programmamanager rapporteert aan het kernteam Datalek (samenstelling op pagina 7)

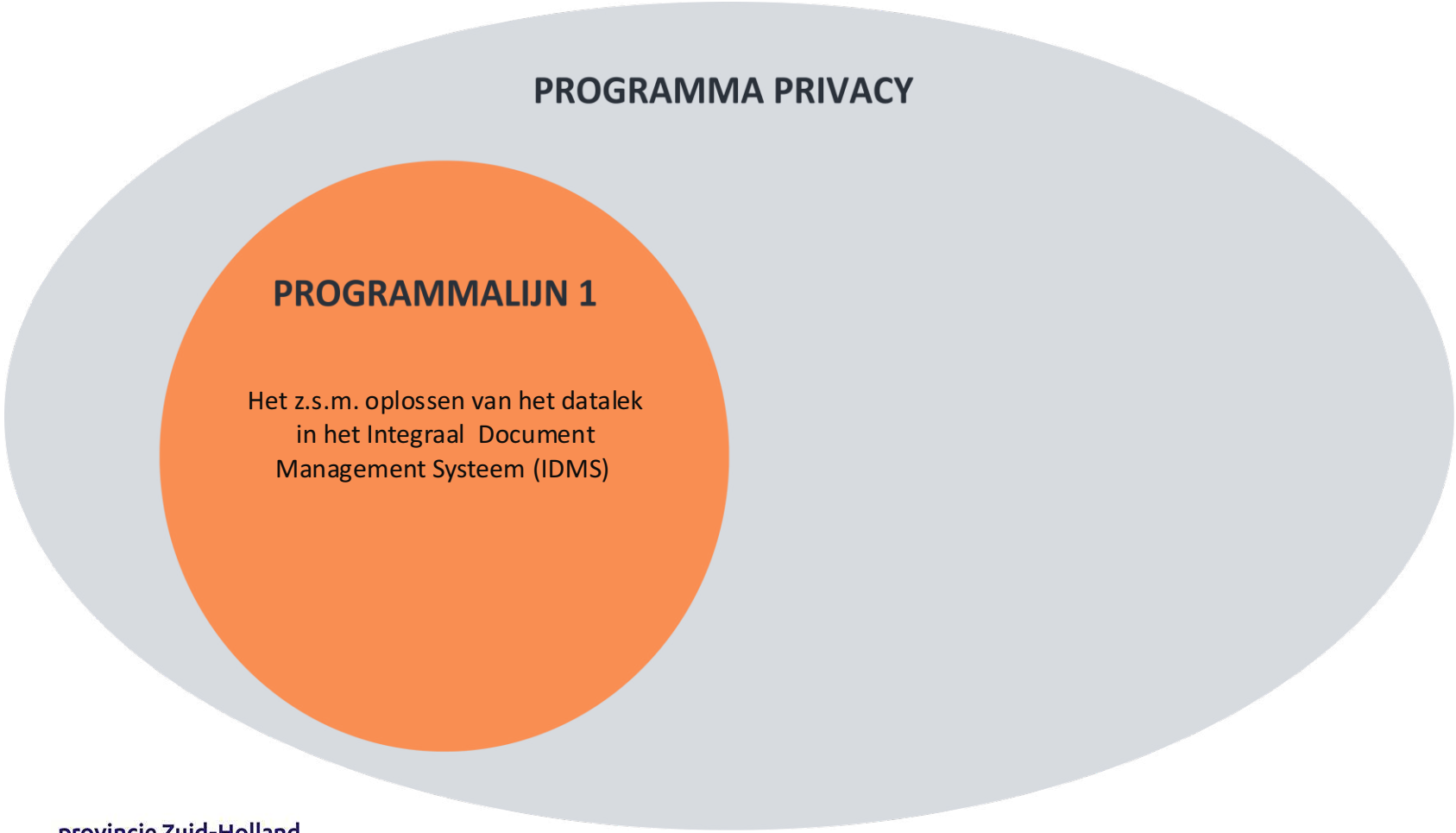
4. Het kernteam besluit over aanpak, en (deel)producten. Strategische beslissingen worden genomen door de stuurgroep.

5. De Informatietransitie is verantwoordelijk voor het technisch dichten van het datalek in iDMS en het realiseren van een (tijdelijke) additionele autorisatiestructuur op het iDMS.

6. Beide programmalijnen kennen een eigen projectteam dat qua samenstelling past bij de betreffende problematiek . Mensen en middelen worden zo pragmatisch mogelijk op basis van risicomanagement ingezet op een wijze waar zij de meeste impact hebben op het verminderen van risico’s in het kader van de bescherming van persoonsgegevens.

Governance


AOG
Concerndirecteur
AON
Directeur bedrijfsvoering
Kernteam
Voorzitter:
Directeur bedrijfsvoering - Sandor Michielse
Deelopdrachtgever:
AOG privacy/ informatieveiligheid - Karel de Wit
Programmamanager privacy - Leandra Beerendonk
AON Informatieveiligheid/ CISO - Laurens van Nes
AON Communicatie - Rowin van der Giessen
AOG Informatietransitie - Marieke van Vonderen
AON Informatietransitie - Anne van Veen
Projectmanager Informatietransitie - Ilona Wansinck
Leandra Beerendonk
Programmalijn 1
Aanpak datalek iDMS
Programmalijn 2
Privacyvolwassenheid
1A
Documenten op orde
Ilona Wansinck
1B
Toegangsrechten op orde
Ilona Wansinck
1C
Informeren betrokkenen
Leandra Beerendonk
2A
Strategisch beleid en governance
Alex Damhuis
2B
Bewustwording
Alex Damhuis
2C
Tactisch- en operationeel beleid en privacy uitvoering
Alex Damhuis


PROGRAMMA PRIVACY
PROGRAMMALIJN 1
Het z.s.m. oplossen van het datalek in het Integraal Document Management Systeem (IDMS)

Inleiding Lijn 1

De Eenheid Privacy ontving op 7 september 2023 een melding van een datalek inzake de applicatie IDMS. Het betreft documenten met persoonsgegevens die breed toegankelijk zijn in iDMS. Uit analyse blijkt dat het iDMS 50,3 miljoen items bevat. Deze zijn als volgt te categoriseren:

1.Centraal toegankelijke documenten:

- Categorie 1: 4,3 miljoen archiefdocumenten
- Deze documenten zijn in het kader van de archiefwet op een specifieke locatie in iDMS gearchiveerd.

- Categorie 2: 7 miljoen ‘oude documenten’
- Deze documenten zijn vanaf 1 augustus 2021 niet meer gewijzigd.

- Categorie 3: 19 miljoen ‘actuele documenten’
- Deze documenten zijn vanaf 1 augustus nog wel gewijzigd en actueel in gebruik.

- **Niet-centraal toegankelijke documenten:**
- Categorie 4: 20 miljoen ‘documenten in persoonlijke mappen’.

Aanpak

De aanpak richt zich in eerste instantie op de 30,3 miljoen items in het centraal toegankelijke deel van iDMS.

- Van een deel van deze documenten (met name ‘archief’ documenten en ‘oude’ documenten) wordt geautomatiseerd de toegang ontnomen (11,3 miljoen items).
- Een ander deel vraagt om geautomatiseerde analyse met de Migrato tooling voordat tot aanpassing van de toegankelijkheid kan worden gekomen (19 miljoen items).

Naar verwachting zullen uiteindelijk ook de 20 miljoen ‘persoonlijke’ documenten worden geanalyseerd om tot een aanpak voor het saneren van de toegankelijkheid te komen

Uitgangspunten en randvoorwaarden Lijn 1

1. De Informatietransitie is verantwoordelijk voor het technisch dichten van het datalek in iDMS en het realiseren van een (tijdelijke) additionele autorisatiestructuur op het iDMS.
2. In aanvulling op de technische oplossing moet ook een structurele verbetering plaatsvinden in bewustwording, houding en gedrag en digitale geletterdheid van alle medewerkers op het gebied van privacy. Dit is onderdeel van lijn 2B.
3. Het technisch dichten van het datalek is een tijdelijke oplossing. Binnen IAM en informatietransitie wordt aan een structurele en duurzame oplossing gewerkt
4. De operatie van de PZH mag zo min mogelijk hinder ondervinden door maatregelen die in iDMS worden uitgevoerd. We accepteren dat medewerkers in sommige gevallen tijdelijk niet over alle benodigde rechten beschikken. We communiceren hierover zo duidelijk mogelijk.
5. Er wordt een nieuwe tijdelijke rechtenstructuur geïmplementeerd. Hierdoor is toegang beperkt tot medewerkers die daar uit hoofde van hun rol 'recht' toe hebben. Helemaal op te lossen is dit punt niet, we zijn namelijk in hoge mate afhankelijk van gedrag. Dit onderstreept het belang van communicatie en training.

Scope

De scope van de aanpak dichten datalek bestaat uit drie elementen:

1A. Documenten op orde

- Met tooling wordt het iDMS doorzocht op documenten met persoonsgegevens. Met deze analyse kunnen we bepalen wie toegang mag hebben tot welke documenten. Zo kunnen we tijdelijk een extra laag toegangsrechten toevoegen aan documenten met privacygevoelige gegevens.
- Twee onderdelen: actuele- en historische documenten

1B. Toegangsrechten op orde

- Er wordt een tijdelijke oplossing geïmplementeerd
- Algemene toegangsrechten worden ingetrokken
- Met de geautomatiseerde analyse kunnen we bepalen wie toegang mag hebben tot welke documenten. Zo kunnen we tijdelijk een extra laag toegangsrechten toevoegen aan documenten met persoonsgegevens.

1C. Informeren van betrokkenen

- Betrokkenen worden omtrent het datalek geïnformeerd conform wettelijke verplichtingen.

Scope 1a: Documenten op orde

In dit deelproject worden historische items veiliggesteld door de rechten van medewerkers te verwijderen.
We analyseren alle documenten in iDMS, classificeren deze en treffen mitigerende maatregelen.

Deel 1: Actuele documenten

Dit omvat een tweetal categorieën:

1. Actuele documenten die recentelijk (na 1 augustus 2021) nog zijn gemuteerd (19 miljoen)
2. Documenten in peroonlijke mappen (20 miljoen)

Deel 2: Historische documenten

Dit omvat een tweetal categorieën:

1. Archief (4,3 miljoen)
2. Items die langer dan 3 jaar niet bewerkt zijn (7 miljoen)

Resultaat: Documenten voldoen aan rechtmatigheidseisen

Aanpak 1a

1. Implementeren Migrato software
2. Analyseren documenten door Migrato, rapportage beoordelen door projectteam Datalek
3. Classificeren documenten
4. Treffen mitigerende maatregelen
5. Helpdesk inrichten
6. Communicatie
7. Autorisaties verwijderen

Met de afdeling Communicatie wordt de interne communicatie afgestemd. Hierbij zal de nadruk liggen op het informeren van de medewerkers waarvan rechten zijn weggenomen. De communicatie zal zo kort mogelijk voor het daadwerkelijk verwijderen van de rechten geplaatst worden op het binnenplein. Dit om te voorkomen dat medewerkers items gaan raadplegen, downloaden en opslaan op een eigen omgeving.

Aanpak 1a (vervolg)

Alle rechten op items in deze deelverzamelingen worden verwijderd, alleen beheerders (functioneel en technisch beheer) krijgen toegang tot de items. In uitzonderlijke gevallen kan een beperkte groep medewerkers geautoriseerd worden, deze toekenning zal in overleg met een privacy officer worden uitgegeven.

De helpdesk wordt geïnstrueerd op meldingen waarin medewerkers aangeven items kwijt te zijn en waarin zij aanvullende autorisaties willen aanvragen. Hiervoor wordt aangesloten op het huidige topdesk proces incl. topdeskformulier. Dit proces wordt met de Eenheid privacy afgestemd. In het proces moet traceerbaar zijn, wie welke aanvullende autorisatie heeft gekregen en op grond waarvan de autorisatie is toegekend.

Alle rechten op items in deze deelverzamelingen worden verwijderd, alleen beheerders (functioneel en technisch beheer) krijgen toegang tot de items. In uitzonderlijke gevallen kan een beperkte groep medewerkers geautoriseerd worden, deze toekenning zal na instemming van de privacy vertegenwoordiger in het project worden uitgegeven. Te denken valt aan de afdeling Kaders, Coaching en Advies die toegang moeten hebben tot het Archief om het archiveringsproces uit te kunnen voeren.

Scope 1B: Toegangsrechten op orde

Implementeren van noodzakelijke additionele rechten op de documenten in scope

1. Alternatieven voor het geautomatiseerd zetten van rechten op documenten in scope
2. Keuze alternatief of combinatie van alternatieven
3. Uitwerking , ontwerp aanvullende rechten, toetsen in een Proof of Concept
4. Inrichten helpdesk voor beantwoorden van vragen en het oplossen van autorisatieproblemen iDMS
5. Inrichten wijzigingsproces m.b.t. toegangsrechten iDMS
6. Realiseren en implementeren aanvullende rechten
7. Inrichten controlerapportage

→ Resultaat: Geïmplementeerde noodzakelijke additionele (beperking van) rechten in iDMS

Scope 1C: Informeren van betrokkenen

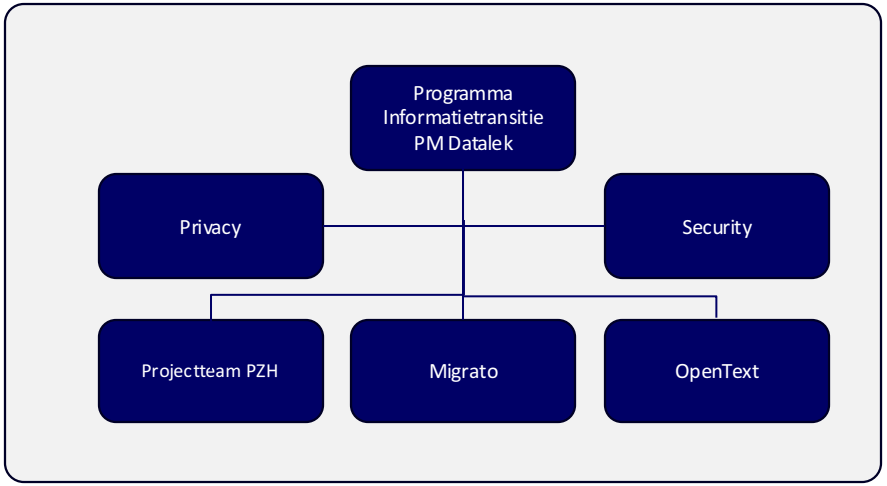
1. Opstellen communicatieplan:
   - Bepalen doelgroepen
   - Boodschap en middelen
2. Uitvoeren communicatieplan
   - Informeren van betrokkenen (breed): betrokkenen waarvan identificatie niet reëel is informeren op bredere wijze
   - Informeren van betrokkenen (individueel indien identificeerbaar) afwegende de noodzakelijke inspanning en vastgestelde privacy impact.
   - Breed communiceren van verwacht gedrag en actie richting organisatie
   - Woordvoering & externe communicatie
3. Evalueren communicatie en waar nodig proces en inhoud bijsturen.

	Centraal deel iDMS		Persoonlijke werkmappen
Totaal iDMS	50,3 miljoen documenten		
Totaal aantal	30,3 miljoen documenten		20 miljoen documenten
Aantal en type documenten	11,3 miljoen 'archief- en oude documenten'	19 miljoen 'actuele documenten'	20 miljoen 'documenten in persoonlijke mappen'
Aanpak	Concern-breed, geautomatiseerd en later geavanceerde analyse door analysetool	Concern-breed, geautomatiseerd na geavanceerde analyse door analysetool	Specifiek, geautomatiseerd na geavanceerde analyse door analysetool en mogelijk na overleg met eigenaar Specifieke aanpak voor deze categorie documenten ontwikkelen we in kwartaal 4 van 2024. Daarna analyse in batches van 4 miljoen documenten begin 2025.

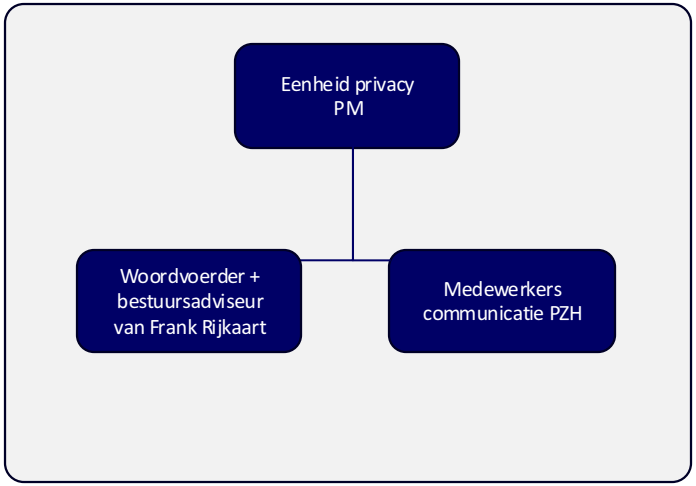
Buiten scope van programmalijn 1 zijn:

1. Inzicht verschaffen in het onrechtmatig gebruik van documenten
2. Het ontwikkelen van een functiemodel inclusief daarbij behorende rechten op documenten en dossiers
3. Implementatie van het (te ontwikkelen) functiemodel in aanvullende rechten op iDMS
4. Ontwikkelen van het proces om tot autorisatiewijziging te komen in doorstroom naar andere functie

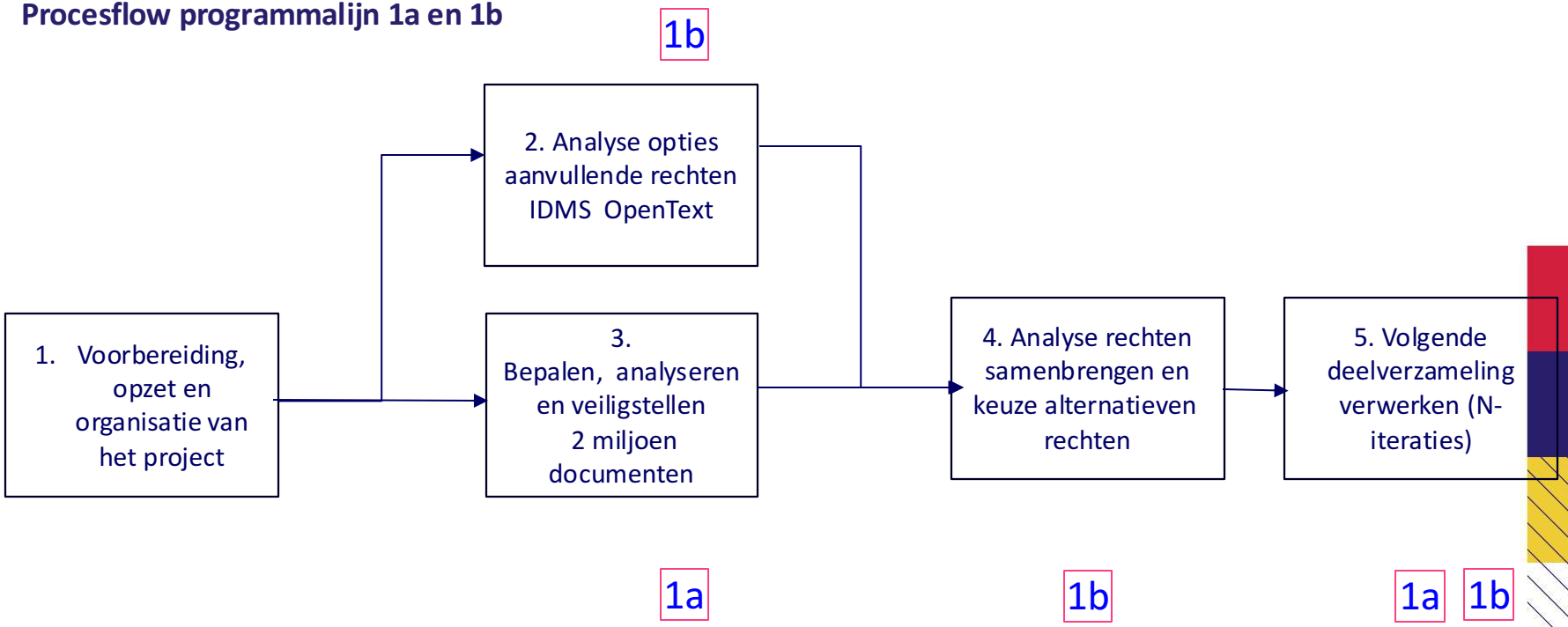
Projectteam 1a en 1b
Onder leiding van Informatietransitie



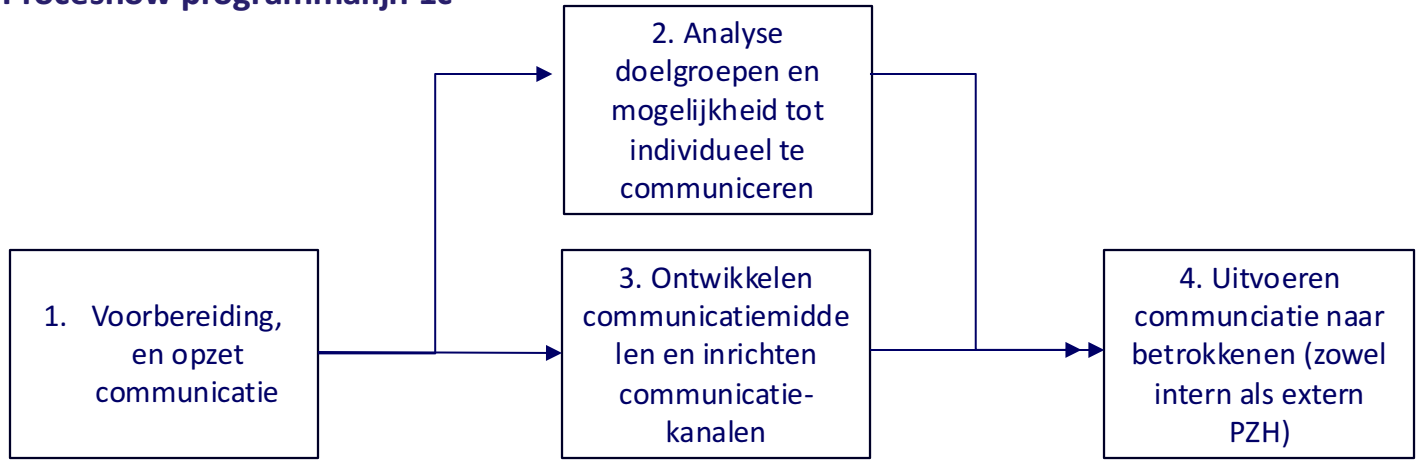
Projectteam 1c
Onder leiding van Eenheid Privacy



Procesflow programmalijn 1a en 1b



Procesflow programmalijn 1c



Resultaten per deelactiviteit programmalijn 1a en 1b Aanpak dichten Datalek (1)

1. Voorbereiding, opzet en organisatie van het project

1. Uitvoeren risicoanalyse’s gebruikte tooling
2. Migrato geïmplementeerd
3. OpenText opdracht gegeven tot analyse
4. Solution Design opgesteld en geaccordeerd
5. Projectteam bemenst
6. Rapportagestructuur ingericht

2. Analyse opties aanvullende rechten IDMS

1. Analyse huidige rechten iDMS door OpenText uitgevoerd
2. Advies OpenText m.b.t. aanvullende rechten

Resultaten per deelactiviteit programmalijn 1a en 1b Aanpak dichten Datalek (2)

3. Bepalen, analyseren en veiligstellen
2 miljoen documenten

Deel 1: actuele documenten

1. Functionele voorbereiding gereed
2. 2 mlj documenten geanalyseerd
3. Advies maatregelen opgesteld
4. Advies Migrato m.b.t. rechten n.a.v. eerste analyse documenten
5. Mitigerende maatregelen uitgevoerd
6. Evaluatie opgesteld incl. Vervolg aanpak beschreven

Deel 2: historische documenten

1. Selectie bepaald
2. Helpdesk ingericht
3. Communicatie strategie bepaald
4. Autorisaties verwijderd

Resultaten per deelactiviteit programmalijn 1a en 1b Aanpak dichten Datalek (2)

4. Analyses rechten samenbrengen en keuze alternatieven rechten

1. Alternatieven opgesteld i.s.m. Migrato - OpenText
2. Keuze uit alternatieven gemaakt
3. Aanvullende rechten in eerste 2 mlj documenten geïmplementeerd

5. Volgende deelverzameling verwerken (N-iteraties)

1. Deelverzameling geanalyseerd
2. Resultaten beoordeeld
3. Maatregelen uitgevoerd
4. Aanvullende rechten gezet

Resultaten per deelactiviteit programmalijn 1C Aanpak dichten Datalek (1)

1. Voorbereiding, en opzet communicatie

1. Uitgangspunten communicatie vastgesteld
2. Communicatieteam aangesteld
3. Planning communicatie vastgesteld

2. Analyse doelgroepen en mogelijkheid tot individueel te communiceren

1. Doelgroepen bepaald inclusief mogelijke ‘risico's'
2. Communicatiestrategie per doelgroep vastgesteld
3. Selectie van personen en organisaties met wie gecommuniceerd wordt (ism PM 1a en 1b)

Resultaten per deelactiviteit programmalijn 1C Aanpak dichten Datalek (2)

3. Ontwikkelen communicatiemiddelen en inrichten communicatie-kanalen

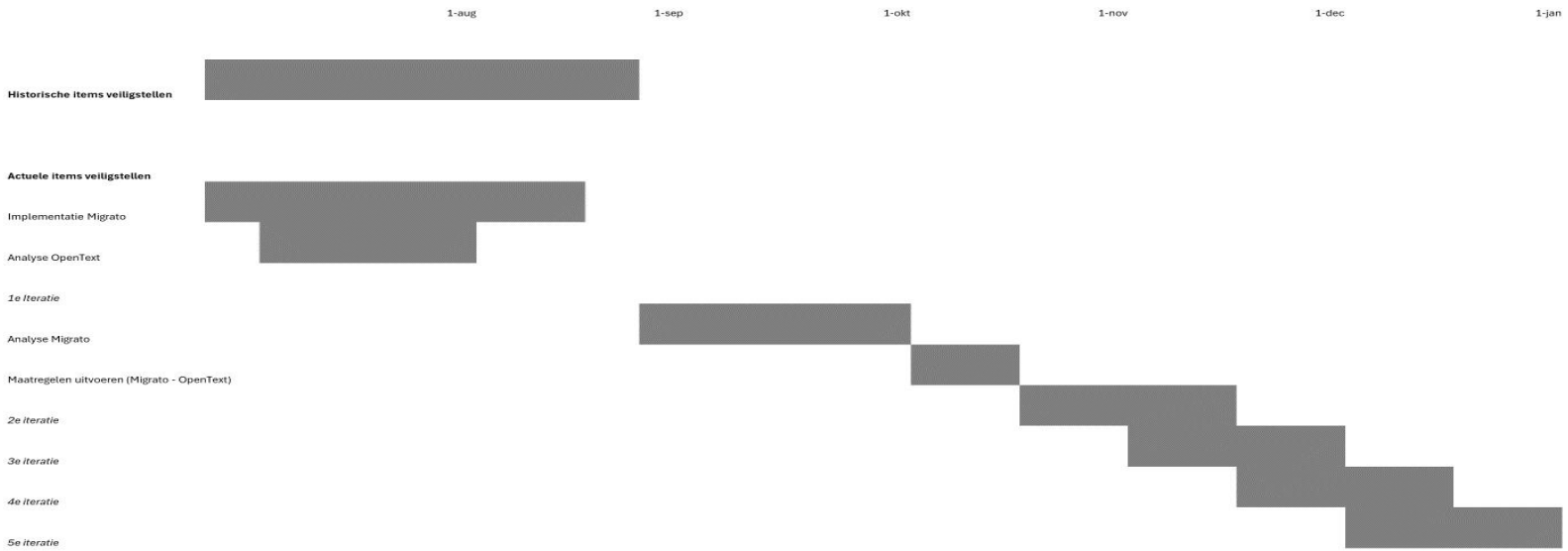
1. Communicatiemiddelen bepaald en ontwikkeld
2. Communicatiekanalen ingericht inclusief de achterliggende (support)organisatie
3. Helpdesk ingericht inclusief de kanalen waarlangs die bereikbaar is
4. Matrix met middelen, kanalen en doelgroepen vastgesteld
5. Vaststellen communicatieplan inclusief planning

4. Uitvoeren communciatie naar betrokkenen (zowel intern als extern PZH)

1. Conform communicatieplan en -planning uitvoeren van de communicatie
2. Evaluatie communicatie
3. Bijsturen communicatie, inclusief planning, doelgroepen, middelen, kanalen en boodschap
4. Conform plan uitvoeren vervolgcommunicatie

Mijlpalen

1a Documenten op Orde en 1b Rechten op orde: deel 1 actuele documenten



Mijlpalen

1a Documenten op Orde en 1b Rechten op orde: deel 2 historische documenten

Mijlpalen:

➢ Selectie bepaald	eind juli
➢ Aanpak geautomatiseerd rechten wijzigen in samenspraak met OpenText	eind juli
➢ Communicatie strategie opgesteld	eind juli
➢ Helpdesk ingericht	eind juli
➢ Eerste groep documenten autorisaties verwijderd	eerste week aug
➢ Autorisaties alle historische documenten (11,3 miljoen) verwijderd	eind sept
➢ PoC Migrato	eind sept
➢ Analyses afgerond 19 miljoen actuele documenten	eind dec
➢ Aanvullende rechten 19 miljoen geïmplementeerd	eind dec
➢ Aanpak 20 miljoen in persoonlijke mappen	eind dec
➢ Analyse 20 miljoen in persoonlijke mappen	n.t.b.
➢ Analyse historische documenten (11,3 miljoen)	n.t.b

Mijlpalen

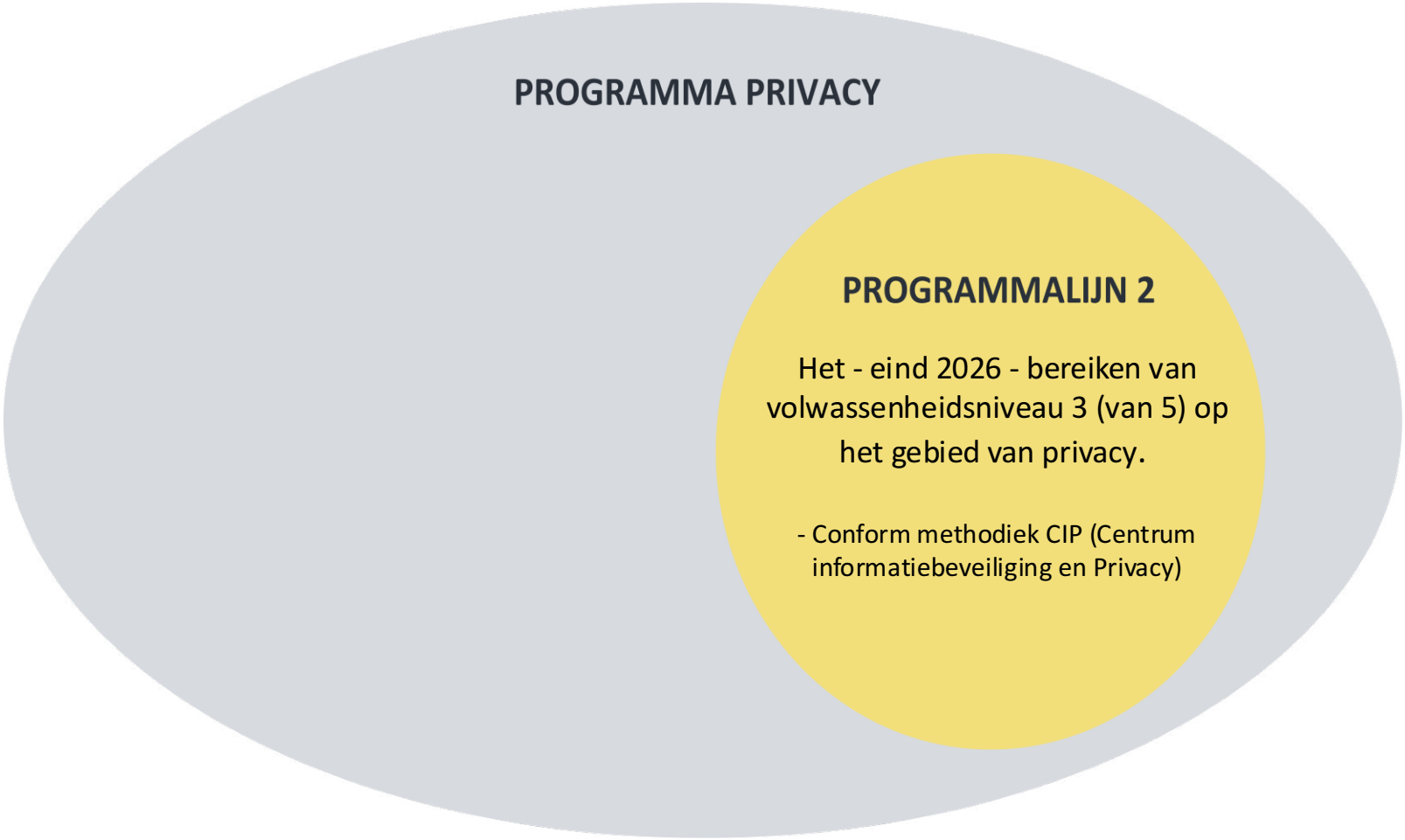
1C Informeren van betrokkenen, organisatie, politiek en media

Mijlpalen

- Uitgangspunten communicatie vastgesteld door EP : Eind juni
- Doelgroepen bepaald inclusief mogelijke ‘risico's' door EP : Eind juni
- Communicatiestrategie per doelgroep vastgesteld : Eind juni
- Communicatieplan vastgesteld : Begin juli
- Uitvoeren van de communicatie : Midden juli

Risico's

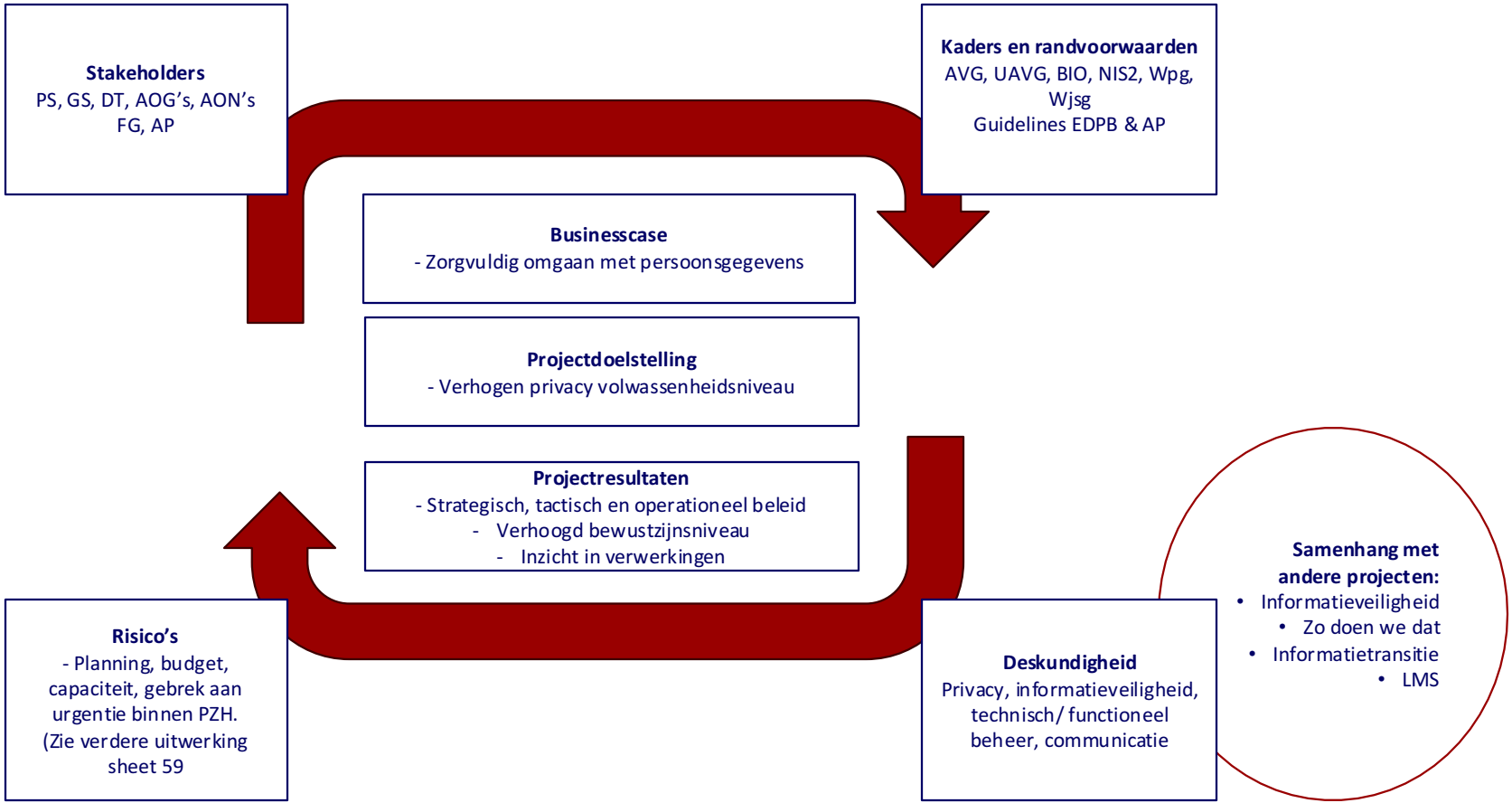
Risico	Impact	Kans	Mitigerende maatregel
Beperkte beschikbare capaciteit vakantieperiodes	Werkzaamheden schuiven naar achteren, planning kan niet gehaald worden	Groot	Inventarisatie vakantieplanning, voor iedere benodigde resource een tweede persoon als achtervang beschikbaar stellen
Resultaten Migrato leveren niet het gewenste inzicht op	Het wordt lastig – zo niet onmogelijk – om per categorie documenten gedifferentieerde mitigerende maatregelen te treffen	Klein	Grofmaziger maatregelen treffen, waardoor grotere groepen gebruikers de toegang tot documenten verliezen (en dus veel individueel beoordeeld moet worden of toegang gerechtvaardigd is
Geen passende aanvullende rechten op basis van de Migrato classificatie	Het wordt lastig – zo niet onmogelijk – om per categorie medewerkers de toegang tot documenten te regelen	Middel	Grofmaziger maatregelen treffen, waardoor grotere groepen gebruikers de toegang tot documenten verliezen (en dus veel individueel beoordeeld moet worden of toegang gerechtvaardigd is
Groepen van medewerkers zijn niet goed te onderscheiden met specifieke rechten (een weinig onderscheidend functiehuis)	Het wordt lastig – zo niet onmogelijk – om per categorie medewerkers de toegang tot documenten te regelen	Middel	Grofmaziger maatregelen treffen, waardoor grotere groepen gebruikers de toegang tot documenten verliezen (en dus veel individueel beoordeeld moet worden of toegang gerechtvaardigd is


PROGRAMMA PRIVACY
PROGRAMMALIJN 2
Het - eind 2026 - bereiken van volwassenheidsniveau 3 (van 5) op het gebied van privacy.
- Conform methodiek CIP (Centrum informatiebeveiliging en Privacy)

Uitgangspunten en randvoorwaarden Lijn 2

1. Privacy is een continu en cyclisch proces op basis van plan-do-check-act, waarvoor het noodzakelijk is om actief vanuit de Opgave en de directie op te sturen.
2. Bescherming van persoonsgegevens is randvoorwaardelijk voor PZH om zijn strategische doelen te behalen en kwaliteit van dienstverlening te behouden. Het vertrouwen van burgers en bedrijven is hier sterk van afhankelijk.
3. de reguliere activiteiten van de eenheid privacy, zoals het adviesvragen, afhandelen van verzoeken, overige datalekken, zullen naast de activiteiten uit dit plan van aanpak worden uitgevoerd.

Programmalijn 2



Privacy volwassenheid

'Privacy volwassenheid' geeft aan hoe volwassen de organisatie is in borging van privacy.

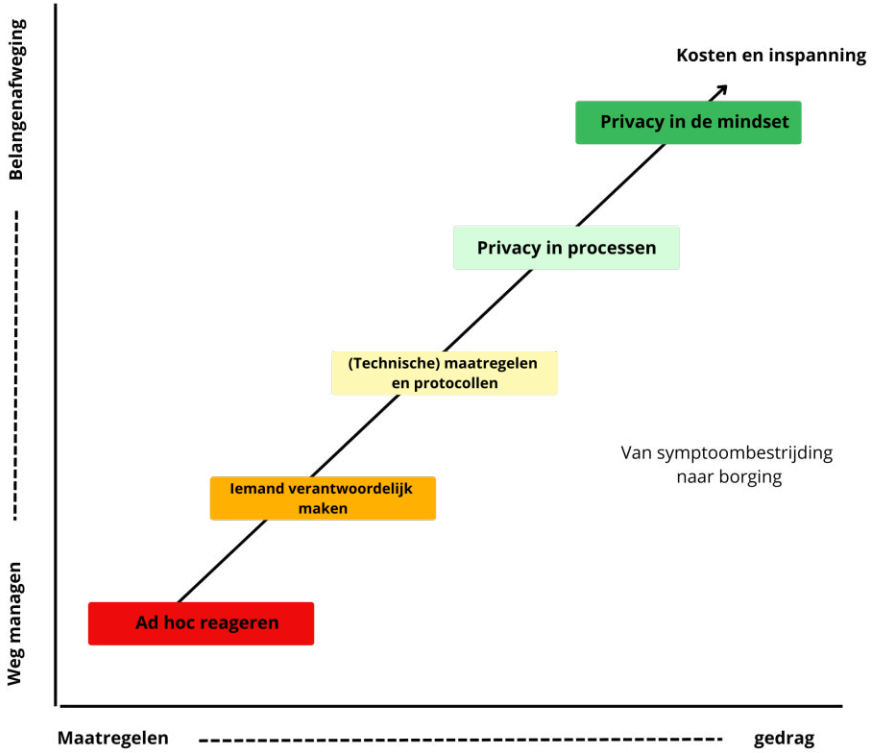
PZH heeft als doelstelling om eind 2025 te voldoen aan volwassenheidsniveau 3. Op niveau 3 werkt een organisatie breed aan privacy en kan dit conform de wet- en regelgeving worden aangetoond.

Gedragsaspecten 1/2

De Privacy Baseline van het Centrum Informatiebeveiliging en Privacy (CIP) geeft een opsomming van normen met bijhorende indicatoren waaraan organisaties moeten voldoen ten aanzien van privacy compliance.

Enkel het treffen van maatregelen voor AVG compliance zoals het implementeren van beleid en uitvoeringskaders, is niet voldoende om gegevensbescherming op volwassenheidsniveau 3 te bereiken.

Daarnaast moet ook worden gekeken naar specifieke gedragingen in de organisatie die wijzen op een bepaalde mate van privacy volwassenheid.



Gedragsaspecten 2/2

Weten: je moet weten wat het nieuwe gedrag inhoudt
Iemand moet bewust zijn van het feit dat er een gedragsverandering gewenst is en het moet duidelijk zijn wat deze verandering inhoudt. Werken aan het aspect ‘weten’ betekent dat je moet inzetten op communicatie en training (Programmalijn 2B).

Willen: je moet je gedrag willen veranderen
Om ervoor te zorgen dat men gemotiveerd is om gedrag te veranderen kan je inzetten op het bespreekbaar maken van het probleem. De medewerker moet begrijpen waarom iets urgent is. Om effectief de intrinsieke motivatie aan te wakkeren is het belangrijk om niet alleen te communiceren in één richting, maar om de dialoog aan te gaan. Zo kan je bijvoorbeeld regelmatig kennissessies organiseren waarbij de discussie centraal staat (Programmalijn 2B)

Kunnen: je moet je gedrag kunnen veranderen
Omdat mensen feilbaar zijn – iedereen is immers wel eens moe of afgeleid - kan je niet uitgaan van verandering vanuit de mens alleen. Je moet er alles aan doen om een omgeving zo in te richten dat het makkelijk is voor de medewerker om zich te gedragen als gewenst. Dit is ook de achterliggende gedachte van het principe ‘Privacy by Design’: wanneer je systemen en processen privacyvriendelijk ontwerpt wordt het makkelijk om privacyvriendelijk te werken (Programmalijn 2C).

→ Het kan zinvol zijn een cultuurscan te laten uitvoeren die inzicht geeft in de huidige (privacy) cultuur binnen PZH en de bijhorende veranderbereidheid. Mogelijkheden hieromtrent wordt binnen programmalijn 2B geïnventariseerd.

Aanpak 1/2

- De AVG geeft slechts een algemeen normenkader en geen concrete handvatten ter invulling daarvan.
- Om te toetsen in hoeverre PZH AVG compliant is, is gebruik gemaakt van thema's. Binnen deze thema's vinden de eisen en normen uit de wetsartikelen van de AVG een plek. Deze thema's zijn ontleend aan o.a. het CIP normenkader en worden ook gebruikt in NORMA: een online toezichtskader welke wij tevens gebruiken als volwassenheidsscan.

Getoetst wordt aan de volgende NORMA-thema's

Thema 1:	Governance
Thema 2:	Register van verwerkingsactiviteiten
Thema 3:	Beleid
Thema 4:	Beleid en operatie
Thema 5:	Bewustwording en opleiding
Thema 6:	Beheersen van informatiebeveiliging
Thema 7:	Beheersen van risico's
Thema 8:	Transparantie
Thema 9:	Rechten van betrokkenen
Thema 10:	Nieuwe verwerkingen
Thema 11:	Managen privacy inbreuken
Thema 12:	Monitoren AVG compliance

Aanpak 2/2

Voor alle thema's is het bruto risico (ofwel de impact van niet naleven voor de organisatie) ingeschat en is een inschatting gemaakt van de mate van naleving om vervolgens het netto risico in te schatten.

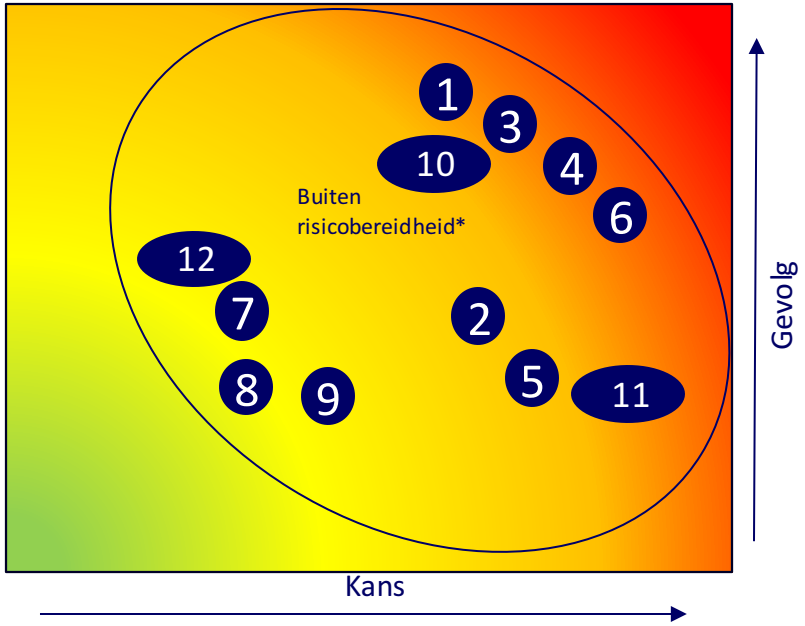
De uitkomsten worden op de volgende pagina weergegeven op een kleurenschaal van laag risico (groen) naar hoog risico (rood). Gebaseerd op het streven om aan volwassenheidsniveau 3 te voldoen, is de risicobereidheid van PZH laag.

Laag risicobereidheid Hoog

Voor de geconstateerde compliance risico's waarbij de netto risico inschatting buiten de risicobereidheid valt, is een prioritering aangebracht. De hoogste risico's krijgen ook een hoge prioritering (deze is terug te zien in de planning). De lager geprioriteerde risico's ten aanzien van AVG compliancy en bijhorende maatregelen ter verbetering zullen volgtijdelijk worden ingezet.

Risicobeoordeling en prioritering

1.	Governance
2.	Register van verwerkingsactiviteiten
3.	Beleid
4.	Beleid en operatie
5.	Bewustwording en opleiding
6.	Beheersen van informatiebeveiliging
7.	Beheersen van risico's
8.	Transparantie
9.	Rechten van betrokkenen
10.	Nieuwe verwerkingen
11.	Managen privacy inbreuken
12.	Monitoren AVG compliance



* De risicothema's binnen de cirkel liggen buiten de vastgestelde risicobereidheid.

Thema's en deelprojecten

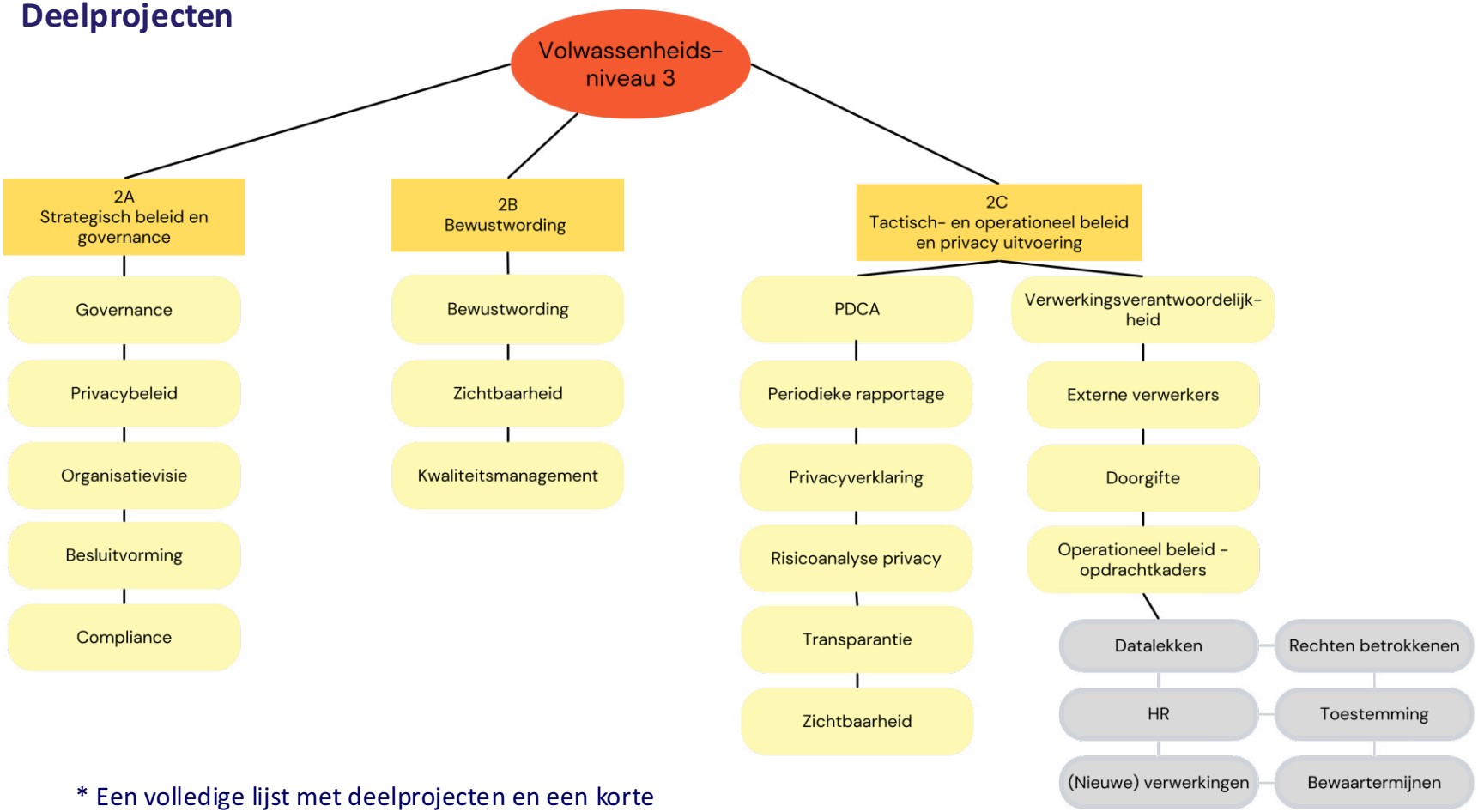
Getoetst wordt aan de volgende NORMA-thema's
(ook zo terug te vinden in de risicoanalyse)

Thema 1:	Governance
Thema 2:	Register van verwerkingsactiviteiten
Thema 3:	Beleid
Thema 4:	Beleid en operatie
Thema 5:	Bewustwording en opleiding
Thema 6:	Beheersen van informatiebeveiliging
Thema 7:	Beheersen van risico's
Thema 8:	Transparantie
Thema 9:	Rechten van betrokkenen
Thema 10:	Nieuwe verwerkingen
Thema 11:	Managen privacy inbreuken
Thema 12:	Monitoren AVG compliance

- De eerder genoemde thema's uit het toezichtskader, worden voor het verhogen van het niveau van privacy volwassenheid, verdeeld in verschillende deelprojecten. Deze deelprojecten zijn op hun beurt verdeeld onder de drie opdrachtlijnen (zie volgende sheets):
  - 2A Strategisch beleid en governance
  - 2B Bewustwording
  - 2C Tactisch- en operationeel beleid en privacy uitvoering.

- Geborgd wordt dat tactisch- en operationeel beleid, richtlijnen en werkinstructies op organisatieniveau aanwezig zijn, en deze tevens zijn vertaald naar de inrichting van systemen en (beheer)processen.
- Daarna kan organisatie breed vorm worden gegeven aan de PDCA-cyclus voor zowel rechtmatige gegevensverwerking (en beveiliging van persoonsgegevens) als het beleid, richtlijnen en (werk)instructies.

Deelprojecten

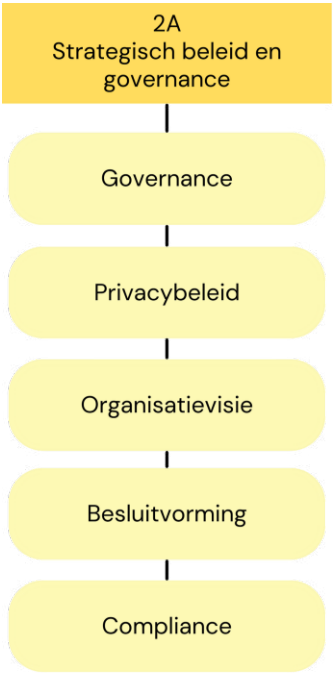


* Een volledige lijst met deelprojecten en een korte toelichting is opgenomen in de bijlage.

2A. Strategisch beleid en governance

Privacybeleid dient ervoor om op organisatie- en strategisch niveau duidelijkheid te geven over de inrichtingskeuzes van privacy en te waarborgen dat de verwerking van gegevens op een rechtmatige wijze plaatsvindt

1. Ontwikkelen organisatievisie op privacy
2. Opstellen strategisch beleidskader conform AVG
3. Ontwikkelen sturingsprocessen en organisatieinrichting (rollen, gremia, rapportage)
4. Implementeren beleidskader
5. Implementeren sturingsprocessen en organisatieinrichting

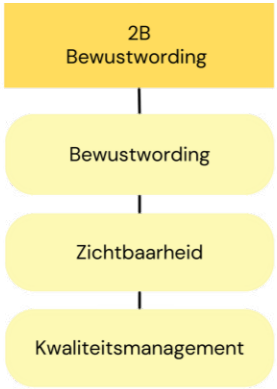


2B. Bewustwording

Bewustwording is essentieel om naleving van privacy wet- en regelgeving te borgen. Dit deel van de scope betreft het informeren, bewustmaken en trainen van bestuur, directie en medewerkers en andere stakeholders: hoe kan een ieder op praktische wijze bijdragen aan de bescherming van persoonsgegevens

1. Informeren van bestuur, directie en medewerkers
2. Bewustmaken bestuur, directie en medewerkers
3. Training van bestuur, directie en medewerkers
   Gedifferentieerd naar rol en mate waarin met persoonsgegevens wordt gewerkt

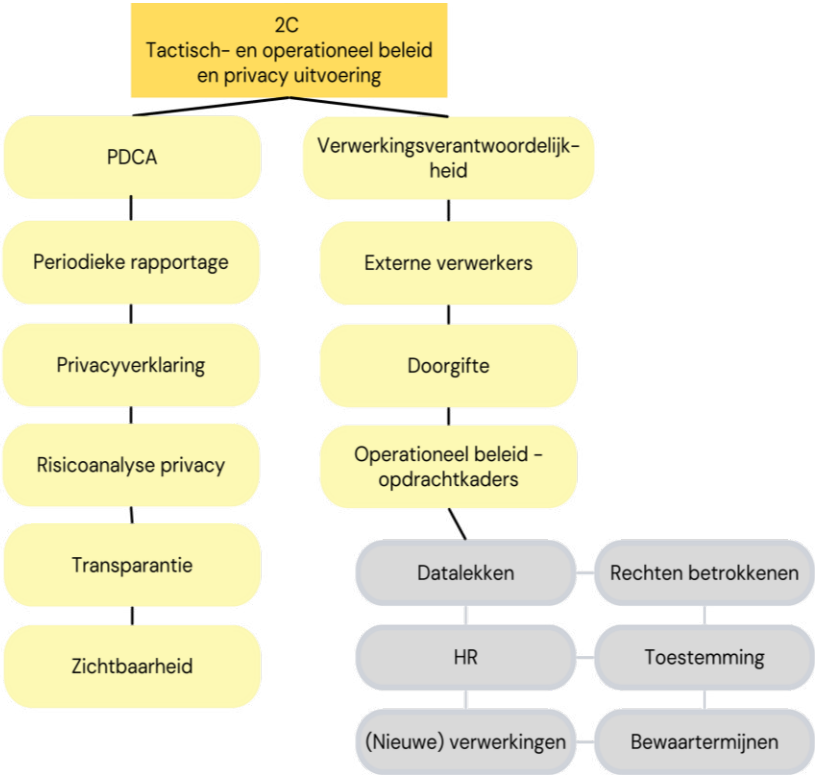
NB 1 uitvoering in samenwerking met opdracht informatieveiligheid



2C. Tactisch en operationeel beleid en privacy uitvoering

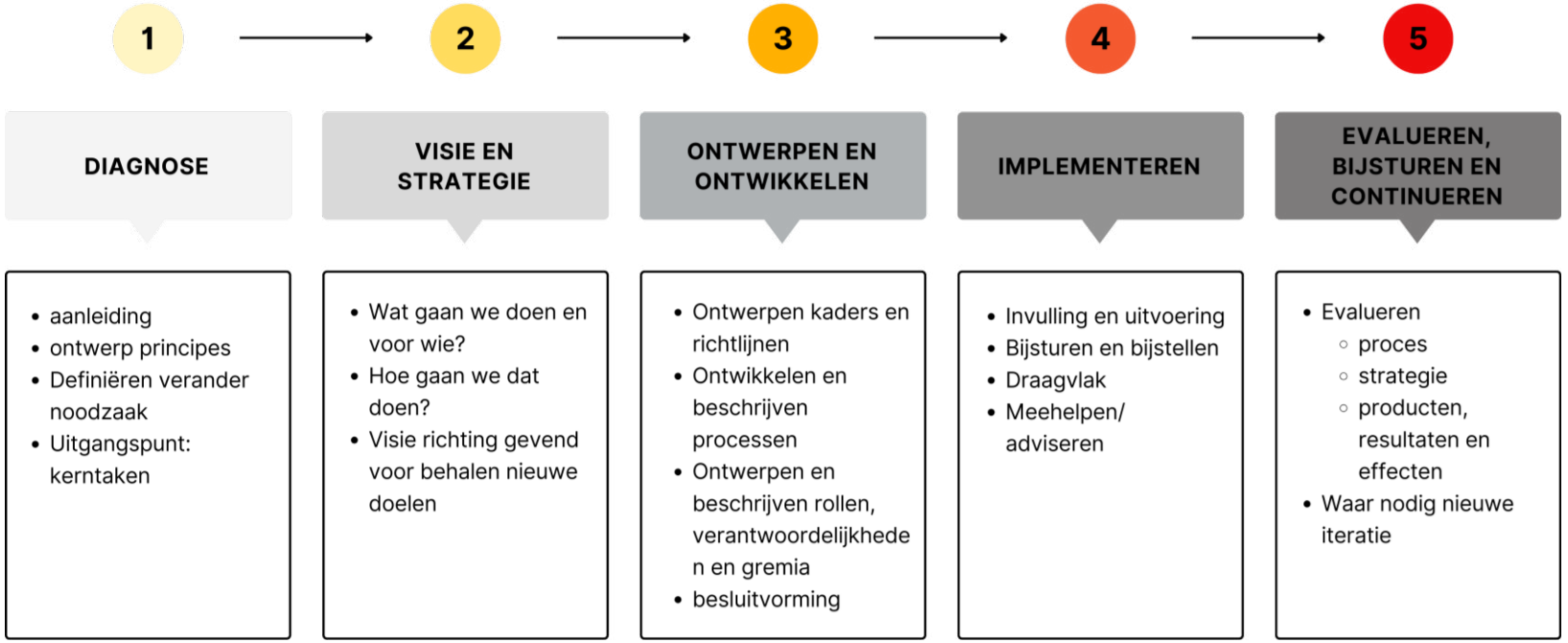
In de uitvoering binnen de domeinen worden persoonsgegevens verwerkt. De verantwoordelijke voor de verwerking moet hier de verwerking realiseren onder de condities en randvoorwaarden die in het strategisch beleid (2a) zijn gedefinieerd

1. Opstellen tactisch en operationele beleidskaders conform AVG
   - Uitvoeringskaders
   - Privacykaders bij opdrachten in domeinen
   - Toezicht- en controleprocessen
2. Implementeren processen en werkinstructies
3. Implementeren sturingsprocessen en organisatieinrichting
4. Inventariseren en uitvoeren noodzakelijke DPIA's
5. Completeren verwerkingsregister
6. Ontwikkelen en implementeren privacy dashboard



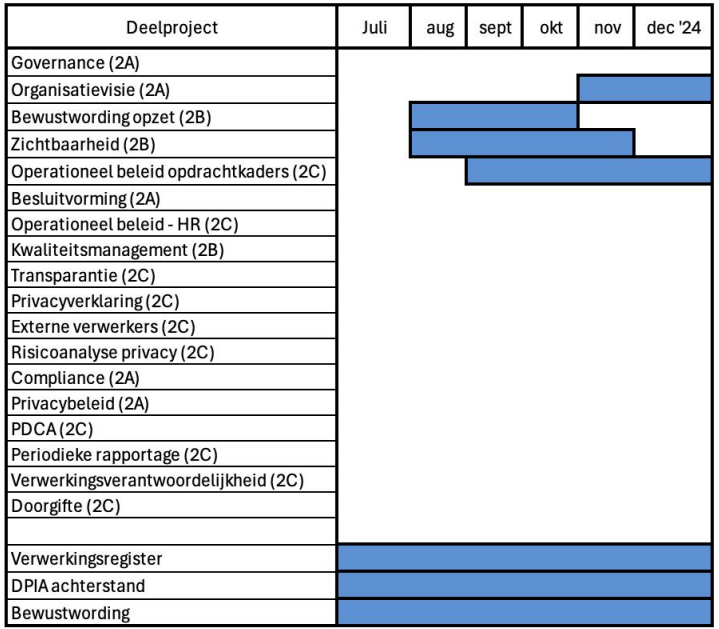
Fasen van deelprojecten

Elk van de beschreven deelprojecten volgt 5 fasen:

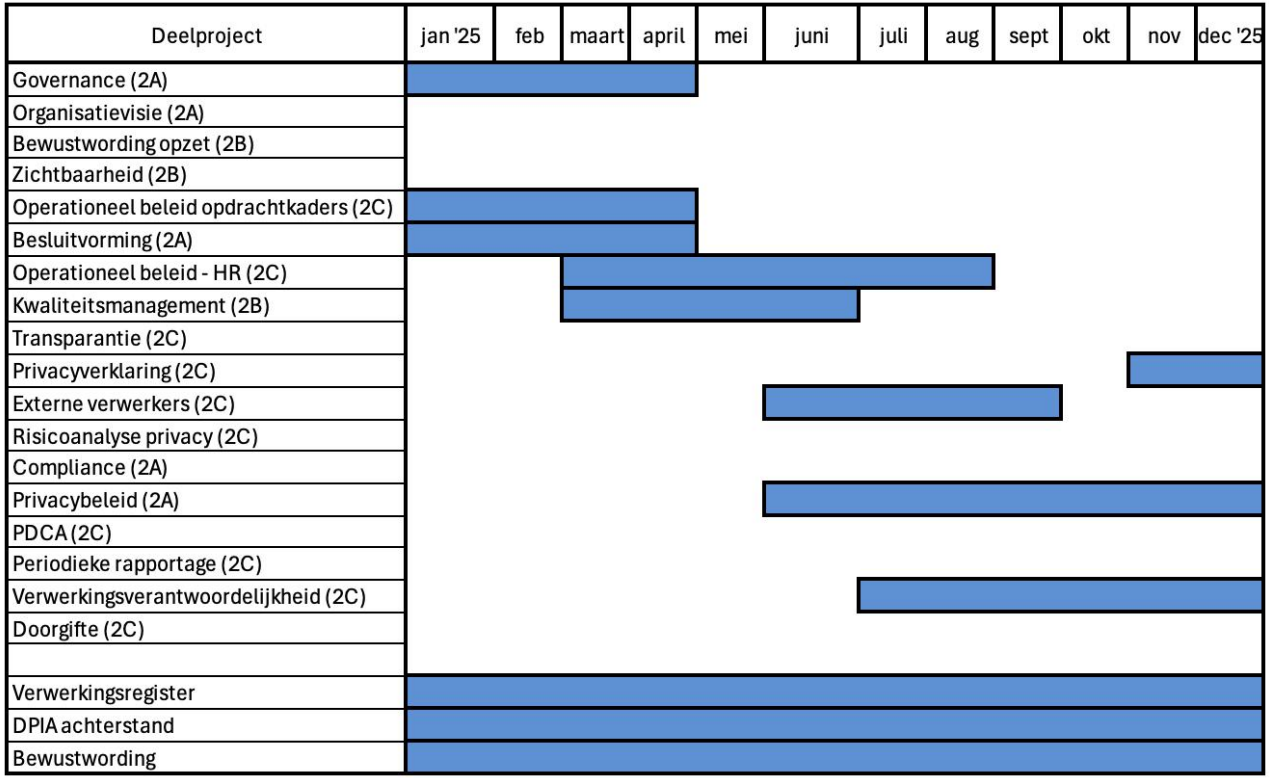


Planning 2024

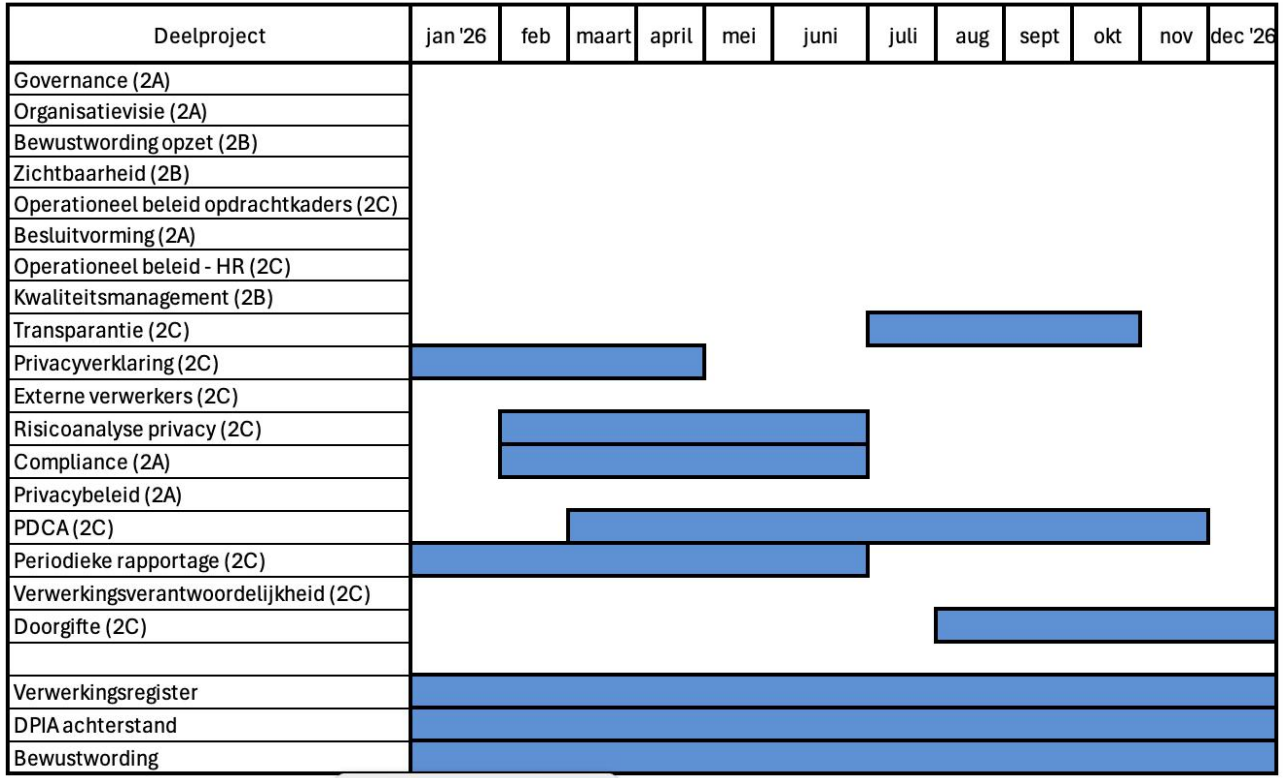
Bij het opstellen van deze planning is nadrukkelijk rekening gehouden met doorlooptijd, beschikbare capaciteit en veranderbereidheid van de organisatie. De planning wordt elk kwartaal geëvalueerd.



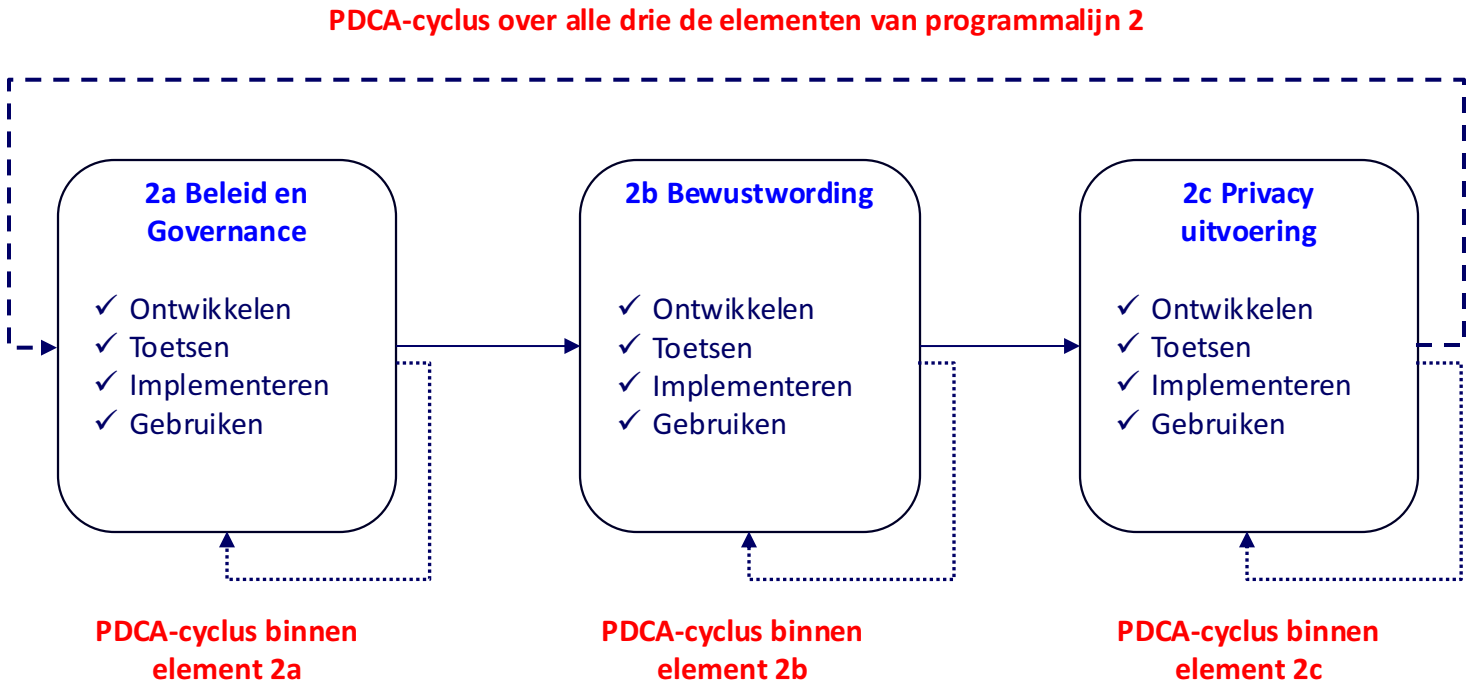
Planning 2025



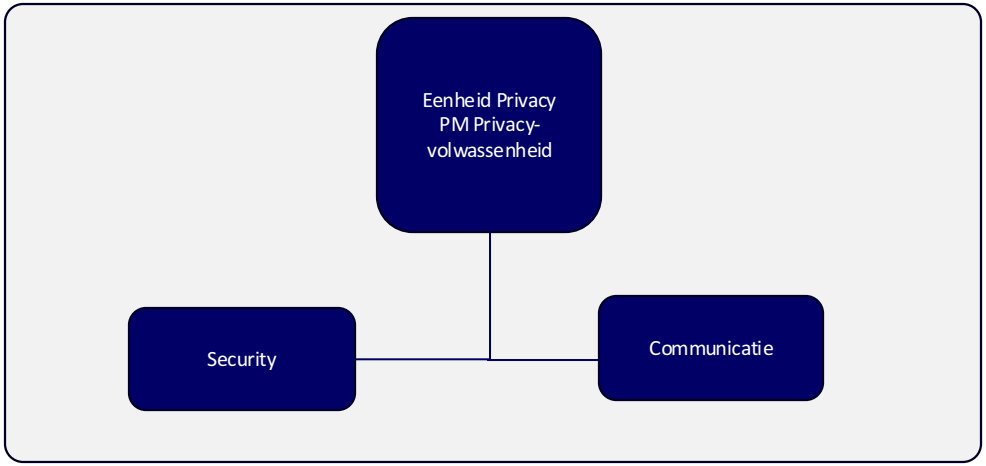
Planning 2026



Dubbele gesloten PDCA-cyclus op het ontwikkelen en implementeren van programmalijn 2



Projectteam lijn 2
onder leiding van eenheid Privacy



Risico's

Risico	Impact	Kans	Mitigerende maatregel
Veranderopgave blijkt te ambitieus	Programmalijn 2 bereikt doelstelling niet (tijdig). Verscherpt toezicht AP blijft in stand	Groot	Planning scherp monitoren en periodiek controleren of planning haalbaar is en waar nodig bijsturen.
Beperkte beschikbare capaciteit	Werkzaamheden schuiven naar achteren, planning kan niet gehaald worden	Groot	Tijdig starten met werving extra capaciteit.
Er is (te) weinig gevoel van urgentie op het gebied van privacy bij bestuur, directie, management en medewerkers	Het bewustzijn op het belang van privacy en de eigen bijdrage daaraan groeit te langzaam. Daarmee blijft PZH langer onder verscherpt toezicht van de Autoriteit Persoonsgegevens staan	Groot	Niveau volwassenheid meten (0-meting, 1-meting etc.) en inzichtelijk maken. Vervolgens meer directief vanuit DT sturen op implementeren en navolgen maatregelen. Gesloten sturingscyclus inrichten en handhaven
Bestuur, directie, management en medewerkers van PZH passen hun gedrag niet aan op het zorgvuldig omgaan met privacygevoelige informatie	Het risico op nieuwe datalekken blijft onverminderd hoog, waardoor het imago van PZH als betrouwbare en zorgvuldige overheid wordt geschaad	Groot	Duidelijk definiëren wat 'gewenst gedrag' is en dit langs diverse kanalen communiceren. Daarnaast het gewenste gedrag via de P-managers en P-teams uitdragen en onderdeel maken van sturing en gesprek over professionaliteit
Het verhogen van het volwassenheidsniveau t.a.v. privacy is te omvangrijk en/of vraagt té veel van de organisatie en komt niet of onvoldoende van de grond	Programmalijn 2 bereikt doelstelling niet (tijdig). Verscherpt toezicht AP blijft in stand.	Groot	Investeren in (externe en professionele) bemensing programmalijn 2. Een 'too little too late'-benadering kan niet in deze programmalijn. Er moet snel en fors worden geïnvesteerd in professionals die deze kar trekken
Er is onvoldoende budget voor het uitvoeren van de opdracht gegevensbescherming en de werkzaamheden die voortvloeien uit het programma.	Programmalijn 2 bereikt doelstelling niet (tijdig). Verscherpt toezicht AP blijft in stand.	Groot	Budgetten moeten zsm beschikbaar worden gesreld

Bijlagen

Deelprojecten lijn 2 Volwassenheidsniveau 1/4

Deelproject	Omschrijving	Actiehouder
(Achterstallige) DPIA's	(Periodieke) uitvoering van DPIA's en ontwikkelen en implementeren proces.	EP
Actualiseren systemen in verwerkingsregister	Eenheid Privacy heeft van het totale verwerkingenbeeld een bijgewerkte schematische weergave op basis van input- en outputstromen.	EP
Actualiseren verwerkingen in verwerkingsregister	Het verwerkingenregister van de organisatie is op een centrale plaats vindbaar, correct gevuld met de voorgeschreven rubrieken en geeft een actueel beeld.	EP
Besluitvorming	Onderdeel van de governance beschrijving is dat de besluitvorming t.a.v. gegevensbescherming op strategisch, tactisch en operationeel niveau, gemotiveerd wordt genomen en gedocumenteerd.	EP
Bewaartermijnen	De organisatie heeft een uitvoeringskader voor het daadwerkelijk uitvoeren en handhaven van bewaar-, verwijder- en vernietigingstermijnen.	EP
Bewustwording en opleiding	Periodiek onderhouden van kennis en awareness van leidinggevenden en medewerkers d.m.v. trainingen. Deze trainingen zijn afgestemd op verschillende interne doelgroepen.	EP
Compliance	Minimaal eens per jaar een interne audit/ compliance check op basis van een auditplan afgestemd op beleid, ambities en jaarplannen. Uitkomsten worden voorgelegd aan verwerkingsverantwoordelijke.	EP
Internationale doorgifte	In geval van doorgifte van persoonsgegevens naar 'derde landen' gebeurt dat o.b.v. passende waarborgen, adequaatheidsbesluiten dan wel bindende bedrijfsvoorschriften.	EP
Externe verwerkers	De organisatie onderhoudt gegevensbeveiligingsvereisten voor derden die in opdracht van de organisatie gegevens van de organisatie verwerken, inclusief procedures voor zorgvuldigheidschecks en niet-nakoming.	EP

Deelprojecten lijn 2 Volwassenheidsniveau 2/4

Deelproject	Omschrijving	Actiehouder
Functionaris voor Gegevensbescherming	Eens per jaar maakt de FG een verslag met daarin een toelichting op het toezicht van afgelopen jaar en een voortuitblik naar het komende jaar. Het verslag vormt de input voor de beleids- en besturingscyclus die de organisatie hanteert en beschreven is in de governance.	FG/EP
Inregelen Governance	Rollen, taken en verantwoordelijkheden zijn vastgesteld, er zijn richtlijnen omtrent gezamenlijke verwerkingsverantwoordelijkheid en het strategisch beleid is uitgewerkt in operationeel beleid.	EP
Informatieveiligheid	Beheersen van informatiebeveiligingsrisico's	IV
Kwaliteitsmanagement	Diplomering, certificering en registratie van medewerkers die een gegevensbescherming accent of specifieke rol hebben wordt structureel onderhouden. De kennis, kunde en toerusting van het management en medewerkers die belast zijn met de uitvoering van processen wordt onderhouden.	EP
Operationeel beleid - Datalekken	De organisatie hanteert een datalekkenprocesure, reageert bij informatiebeveiligingsincidenten en datalekken, aantoonbaar adequaat en neemt waar van toepassing direct maatregelen om (verdere) gevolgen te stoppen of te beperken. Crisiscommunicatie maakt daar deel van uit.	EP
Operationeel beleid - HR	Uitvoeringskaders omtrent screening en geheimhouding, gebruik van social media en gedragscodes.	EP
Operationeel beleid - Nieuwe verwerkingen	Bij de aanschaf van systemen en producten en in de ontwikkeling en aanpassing van systemen, processen en procedures wordt, conform het daartoe ontwikkelde proces en de governance beschrijving, van geval tot geval een check gedaan of de voorgenomen verwerkingen compliant en conform het beleid van de organisatie zijn. Daarbij inbegrepen het uitvoeren van pre-DPIA's, opvragen FG-advies en het hanteren van privacy by design.	EP
Operationeel beleid - Opdrachtkaders	De organisatie hanteert algemene op de werkvloer toepasbare uitvoeringskaders, waarin is beschreven hoe de verplichtingen en de beginselen die de AVG koppelt aan het verwerken van persoonsgegevens in het dagelijks werk toegepast moeten worden.	EP

Deelprojecten lijn 2 Volwassenheidsniveau 3/4

Deelproject	Omschrijving	Actiehouder
Operationeel beleid - Rechten betrokkenen	De organisatie heeft en onderhoudt een procedure die beschrijft hoe de afhandeling van verzoeken, klachten en bezwaren compliant en binnen de wettelijke termijnen uitgevoerd worden. En de organisatie heeft haar processen zodanig ingericht dat gegronde verzoeken van betrokkenen daadwerkelijk worden uitgevoerd.	EP
Operationeel beleid - Toestemming	Daar waar bij een verwerking van persoonsgegevens sprake is van de wettelijke grondslag 'toestemming' van de betrokkene is dat nadrukkelijk, aantoonbaar en reproduceerbaar gedocumenteerd en er is een proces ingericht om te waarborgen na gegevens na het intrekken van toestemming niet meer worden verwerkt.	EP
Operationeel beleid - Verwerkingen	De organisatie heeft een intern proces aan de hand waarvan het verwerkingenregister onderhouden wordt. Alle processen zijn inzichtelijk en hebben een proceseigenaar. Er is een werkwijze ingericht voor het up-to-date houden van het register van verwerkingen.	EP
Organisatievisie op privacy	Er is een door het Bestuur, de Directie en het MT geaccordeerde en actuele organisatievisie, -aanpak en/of -strategie m.b.t. privacy en gegevensbescherming. Dit is nader uitgewerkt in het privacy beleid en informatiebeveiligingsbeleid. Onderdeel daarvan is het risico acceptatiebeleid.	EP
PDCA	Er is sprake van een projectmatige, programmatische of lifecycle aanpak van de verbeter-, leer en groeipunten m.b.t. privacy en gegevensbescherming. De sturing op voortgang privacy en informatiebeveiliging o.b.v. beleid en jaarplannen, alsmede tactisch en operationeel risicomanagement maakt onderdeel uit van de reguliere besturingscycli die de organisatie hanteert. In die zin is sprake van eigenaarschap.	EP
Periodieke rapportage	De in- en externe stakeholders zijn en worden, conform hetgeen daarover is afgesproken en vastgelegd, actief betrokken bij de onderwerpen privacy en gegevensbescherming en er wordt periodiek aan hen gerapporteerd. In de governance is beschreven wie daarin welke rol, taak en verantwoordelijkheid heeft.	EP
Privacyverklaring	De organisatie onderhoudt een privacyverklaring die de verwerking van persoonsgegevens van betrokkenen door de organisatie in begrijpelijke taal en op de betrokkene(n) gericht, vermeldt.	EP
Strategisch beleid	Het privacybeleid en het informatiebeveiligingsbeleid van de organisatie is conform de governance tot stand gekomen. Dit beleid maakt onderdeel uit van de beleidscyclus die de organisatie gebruikt en er is bij vaststelling ervan een belangenafweging gehanteerd, gebaseerd op zowel morele als juridische waarden.	EP

Deelprojecten lijn 2 Volwassenheidsniveau 4/4

Deelproject	Omschrijving	Actiehouder
Risicoanalyse privacy	Voor het besturen en ontwikkelen van privacy en gegevensbescherming bedient de organisatie zich periodiek (bijvoorbeeld per kwartaal) van een risicoanalyse op het gebied van beide onderwerpen, op zowel strategisch, tactisch als operationeel niveau. De uitkomsten zijn over en weer input voor elkaar. Privacy en gegevensbescherming worden zoveel mogelijk integraal opgepakt.	
Transparantie	De organisatie publiceert haar register van verwerkingsactiviteiten, toezichtverslagen en audituitkomsten; heeft haar procesgang zo ingericht dat de betrokkene, (indien wettelijke verplicht) vooraf in kennis wordt gesteld van relevante wijzigingen in de verwerking van persoonsgegevens en onderhoudt een FAQ om op vragen van betrokkenen te reageren.	EP
Verwerkingsverantwoordelijkheid	De juridische verwerkingsverantwoordelijkheid is op basis van een interne mandaatregeling met meerdere functionarissen nader ingeregeld. Zo kennen alle werkprocessen proceseigenaren en zijn leidinggevenden bekend met het beleid en de jaarplannen privacy en gegevensbescherming en dragen dit actief uit.	EP
Zichtbaarheid	Er is een specifiek privacy nieuwsmedium aan de hand waarvan de leidinggevenden en medewerkers t.a.v. worden geïnformeerd. Voor de uitvoering is een ‘hulpstructuur’ in de governance beschreven en operationeel.	EP