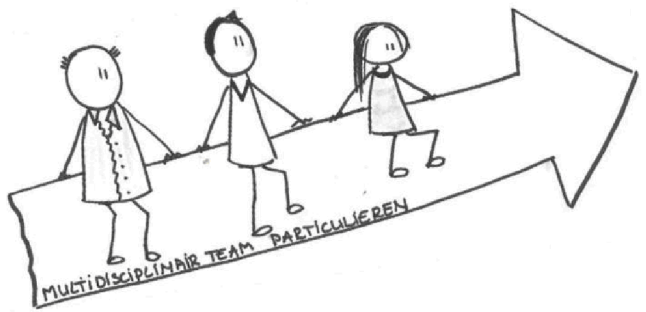
IN CONTROL STATEMENT PARTICULIEREN

COMPLIANTIE TOETS – BEVINDINGEN

Programma ICS-P ⇔ Ketenmanagersoverleg



23 september 2023

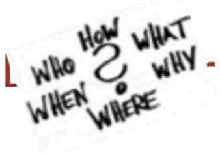
Leeswijzer

Deze presentatie bestaat uit 4 onderdelen die zelfstandig leesbaar zijn. Om de leesbaarheid te bevorderen is gebruik gemaakt van iconen, je kan zo snel en eenvoudig binnen de onderdelen van de presentatie switchen in plaats van de gebruikelijk ↑↓ toetsen.

Inhoudsopgave op de dia (voorbeeld):

Door hier op te klikken ga je direct naar de betreffende dia

Rechtsboven op de dia (voorbeeld):



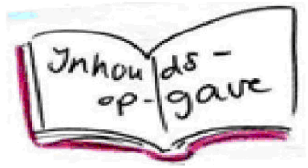
- op te klikken ga je terug naar de dia van het betreffende onderdeel

Rechtsboven op de dia (voorbeeld):

Als een onderdeel uit meerdere dia's bestaat kan je voor- of terugbladeren m.b.v. deze iconen

Inhoudsopgave

Samenvatting MDT-P voor KM overleg



Inhoudsopgave presentatie rapportage MDT-P

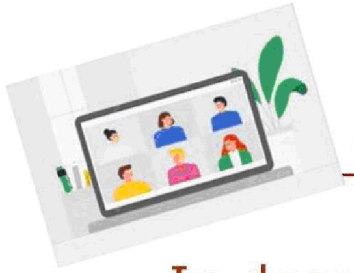
Inleiding

MDT-P Stappen uitgevoerde toets AVG, BIO en AW

Managementsamenvatting bevindingen

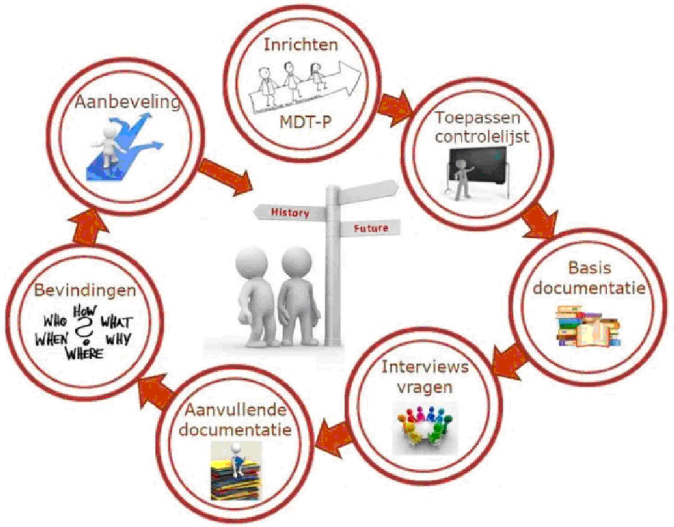
Bijlage: samenvatting bevindingen

Samen verbeteren

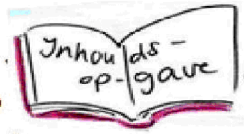


Samenvatting voor KM overleg (1/3)

- In december 2022 – mei 2023 3 bedrijfsprocessen in de volle breedte en diepgang aan de hand van de controlelijst getoetst voor:
  - Keten IH aanslag : bedrijfsproces [IH] Opleggen ambtshalve
  - Keten S&E erfbelasting : bedrijfsproces [EB] Afhandelen aangifte
  - Keten BBK : bedrijfsproces [BZ] Behandelen Bezwaar IH
- Samenstelling vaste kern inhuur en een vaste medewerker, flexibele schil zijn BD medewerkers
- Algemeen is er vriendelijkheid en openheid over het onderwerp. Er wordt ruimte gemaakt in agenda's zonder TWR codes vooraf en achteraf
- Interviews en/of sessies bij aanvullende vragen



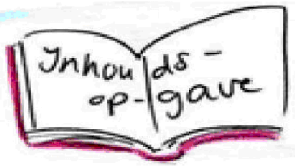
Samenvatting voor KM overleg (2/3)



Geleerde lessen:

- Basisdocumentatie is niet voldoende
- Bevindingen bespreken / afstemmen (hoor en wederhoor) (binnen en buiten de eigen keten / domein)
- Investeer in kennis van het voortbrengingsproces (Gevraagde inzet IV&D 25 uur / IV 18 uur bij de 3 BP)
- Controlelijst bekijkt aspecten van een bedrijfsproces en vraagt om aanvullingen
- De geconstateerde omissies binnen de opzet en bestaan van één bedrijfsproces zijn gelijk gebleken bij het toetsen van het volgende BP binnen de keten maar ook bij een BP van een andere keten
- De structurele oplossing in de huidige opzet van de verticale data architectuur (VDA) geeft nog niet voldoende inzicht in het verwerken, corrigeren, verwijderen en inzien van gegevens op procesniveau.

Samenvatting voor KM overleg (3/3)



Hoe verder:

- Gepland BP geclusterd per domein controlelijsten opstellen
- Gaan voor de verbetering een MDT 2.0 inrichten met alle deskundigen van alle betrokken stakeholders (verwachting medio oktober)
  (beginnen casus bij BP Afhandelen Aangifte [EB])
- Communicatie via de lijn van de keten (Ketentafel, ketenmanagers, ketenvoorzitters)

Doel en grondslag verwerken gegevens BP
- Bij hoog risico privacy uitvoeren DPIA
- Privacy by design
- Need to know

Gemodelleerde gegevens

Het datamodel is gemodelleerd op een keten of bedrijfsproces, vanuit de VDA principes met toepassing op een werkproces

Het werkproces of processtap

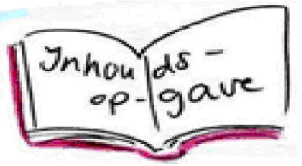
De processtap binnen een werkproces in een schematische weergave (procesmodel AO)

Metadata van de relatie tussen data, processen en regels
- welke type gegevens wordt gewerkt
- Grondslag gebruik gegevens
- Verwerkingsregister
- Type verwerking
- (Onderdeel van) een informatieobject
- Archiefwaardig?

Doel: samen komen tot een MTHV die de gegevens en bedrijfsprocessen in één schema modelleren met als doel aantoonbaar compliant te zijn in opzet en bestaan.

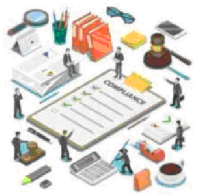
Vragen (?)

Inhoudsopgave bevindingen MDT-P



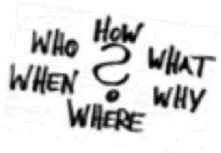
1. Inleiding

2. MDT-P Stappen uitgevoerde toets AVG, BIO en AW



3. Managementsamenvatting bevindingen

Bijlage: samenvatting bevindingen



4. Samen verbeteren

1. Inleiding

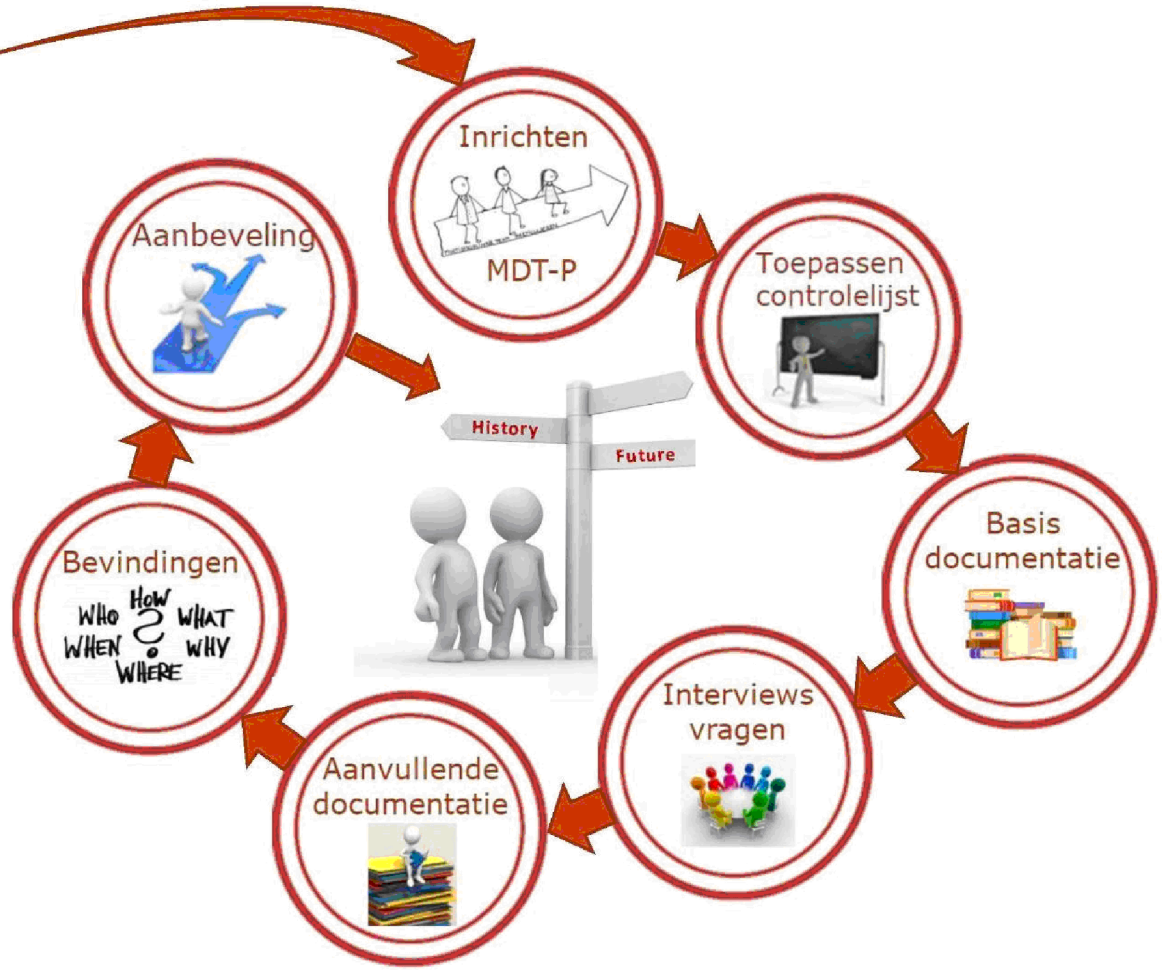
In de driehoek IV&D van 13 mei 2022 is afgestemd dat de focus in 2022 bij de aanpak en uitvoeren van de toets op de compliantie voor de Algemene Verordening Gegevensbescherming (AVG), de Baseline Informatiebeveiliging (BIO) en de Archiefwet (AW) ligt bij de meest risicovolle bedrijfsprocessen. De sturing en de rapportage op de voortgang van de toets op de compliantie loopt via de via de stuurgroep ICS (In Control Statement).

Na uitvoeren van de pilot MDT (juli '22) en op basis van de aanbevelingen stuurgroep ICS (9 sep '22) heeft de directie P haar MDT-P in 4e kwartaal 2022 ingericht met een vaste kern (3 fte inhuur en 2 fte vast) en een flexibele kern. Capaciteit voor de flexibele kern is in het portfolio 2023-2024 van de ketens (IH, S&E en BBK) opgenomen.

Het MDT-P is vanaf medio november 2022 operationeel. Doel van het MDT-P is het uitvoeren van de toets op de compliantie voor de hoog risicovolle bedrijfsprocessen via de ketenlijn. Als aanpak is gekozen om dit al lerend te ontwikkelen en te zorgen dat in de 1ste helft van 2023 in ieder geval een hoog risicovol bedrijfsproces van de ketens IH, BBK en S&E te hebben getoetst en uiterlijk mei '23 deze aanpak te evalueren.

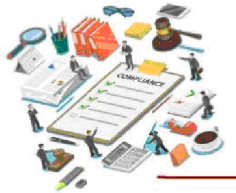
Eind mei 2023 heeft het MDT-P 3 bedrijfsprocessen afgerond op basis van afstemmingen met de flexibele kern (kaderstellers, referentie architect, domein architect, informatie architect en korte afstemmingen met vele collega's in het werkveld). In dit document zijn de bevindingen van het MDT-P, de vervolgacties op basis van deze bevindingen en de aanpak voor het vervolg binnen de ketens IH, S&E en BBK opgenomen.

2. MDT-P: Stappen toets AVG, BIO en AW



MANAGEMENTSAMENVATTING

BEVINDINGEN MDT-P



3. Managementsamenvatting

In de periode december 2022 – mei 2023 heeft het MDT-P de volgende 3 bedrijfsprocessen in de volle breedte en diepgang aan de hand van de controlelijst getoetst:

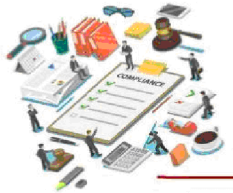
- Keten IH : bedrijfsproces [IH] Opleggen ambtshalve aanslag
- Keten S&E : bedrijfsproces [EB] Afhandelen aangifte erfbelasting
- Keten BBK : bedrijfsproces [BZ] Behandelen Bezwaar IH

De aanpak voor de toets is bij de 3 ketens uniform gebleven. Bij het uitvoeren van de toets is naast collegiale afstemming (belastingdienst breed) ook regelmatig afstemmingen geweest met de kaderstellers, referentie-, domein- en informatie architect over de antwoorden en geconstateerde omissies.

Bij het uitvoeren van de toets en de gehouden interviews is een rode draad te zien in de bevindingen en geconstateerde omissies AVG, BIO en AW binnen de 3 ketens. Aanleiding voor het MDT-P om verder te onderzoeken of:

a. de omissies voor het gehele domein gelden;
b. bij de verbetertrajecten voor nieuwe functionaliteiten of bij nieuwe systemen de geconstateerde omissies zijn aangepakt.

De aanvullende onderzoeken tonen aan dat de geconstateerde bevindingen bij het toetsen van het bedrijfsproces niet specifiek voor één bedrijfsproces opgaan maar dat deze bevindingen gelden binnen het gehele domein van de keten.



3. Managementsamenvatting (vervolg)

In de bijlage zijn de bevindingen gedetailleerder opgenomen, hoog over zijn de geconstateerde omissie als volgt:

> " In de huidige documentatie van procesontwerpen, datamodellen, administratieve organisatie en (wettelijke) uitvoeringsrichtlijnen is geen onderlinge relatie bij het kunnen inzien, verwerken, corrigeren, verwijderen en beperken van persoons- en bijzondere persoonsgegevens. Daarnaast beoordeelt de controlelijst niet integraal de compliantie op AVG, BIO en archiefwet."

Het dossier van de door het MDT gebruikte documenten, analyses, bevindingen en geconstateerde omissies zijn opgeslagen in een CP omgeving die overdragen kunnen worden aan de keten- en lijnorganisatie.

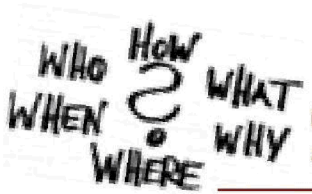
De geconstateerde omissies binnen de opzet en bestaan van de bedrijfsprocessen zijn te groot om met behulp van "pleisters" tijdelijk op te lossen. De structurele oplossing in de huidige opzet van de verticale data architectuur (VDA) geeft nog niet voldoende inzicht in het verwerken, corrigeren, verwijderen en inzien van gegevens op procesniveau.

Het organiseren van de status en de ontwikkeling van niet fiscale wet- en regelgeving in een multidisciplinair team bij de keten is aan te bevelen.

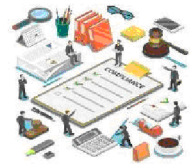
De bevindingen en conclusie van het MDT-P is door de directie afgestemd met onder meer de directie IV, Keten Gegevens, IH, S&E, BBK en cd IV&D. Uit deze afstemmingen zijn geen andere inzichten en bevindingen na voren gekomen (geschetste beeld is herkenbaar).

MANAGEMENTSAMENVATTING

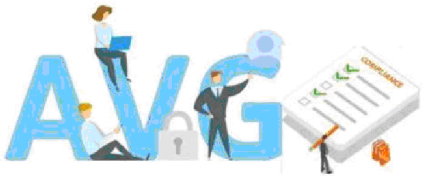
BIJLAGE: SAMENVATTING BEVINDINGEN MDT-P



Samenvatting bevindingen



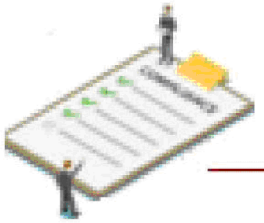
Samenvatting gebruik controlelijst



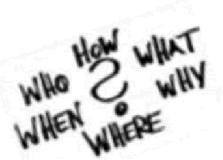
Samenvatting bevindingen AVG

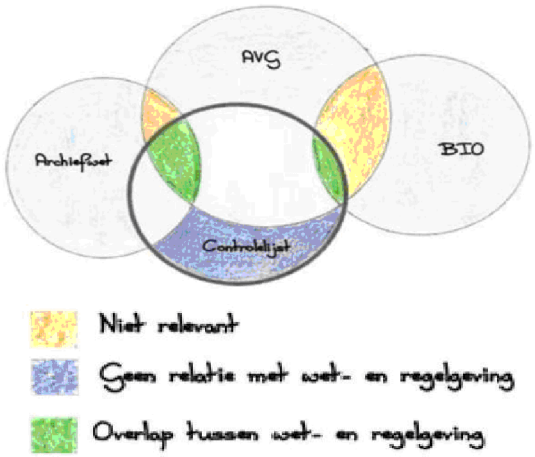
Samenvatting bevindingen overig

Bijlage: bevindingen BIO (werking)



3. Samenvatting bevindingen: controlelijst

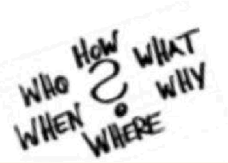




- Bedoeld als tijdelijke maatregel voor AVG, BIO en archiefwet terwijl structurele oplossingen ontwikkeld zouden worden.
- Bedoeld om inzicht te krijgen in compliantie bedrijfsprocessen
- Controlelijst bekijkt aspecten van een bedrijfsproces en vraagt om aanvullingen:
  - Voorbeelden zijn dan onderdelen uit de AVG en de archiefwet:
    - AVG: Kinderen onder de 16, nationaliteit (bijzondere persoonsgegevens)
    - Archiefwet: plaats informatieobjecten en actualiteit vernietigingsverklaring
- Er is geen sprake van een volledige compliantie als de controlelijst wordt doorgevoerd.

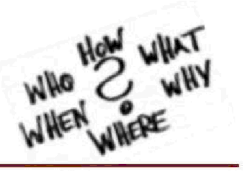
- Wat er niet is vastgelegd, maak daar een GAP lijst van als activiteit om in 2 jaar aantoonbaar compliant te zijn, ***maar:***
  - Er ontbreekt teveel om aanvullingen te doen, er ontbreekt een ontvangende (infra)structuur om verbeteringen in aan te brengen en er ontbreekt een control framework
  - Het is te omvangrijk en te onbeheerst om elk bedrijfsproces af te lopen en aan te vullen. Alles moet worden aangevuld.
  - De afhankelijkheden tussen de verantwoordelijkheden binnen en buiten de keten voor de thema's in de controlelijst zijn complex

Samenvatting bevindingen AVG



- Persoonsdata wordt niet geclassificeerd als zodanig in documenten als domein- en solution architectuur
- Er wordt geen relatie gelegd tussen werkprocessen en (persoons)gegevens en daarmee ontbreekt ook de basis voor compliantie.
- Het verlenen van fysieke toegang in applicaties tot verwerking van persoonsgegevens is niet gedocumenteerd
- De primaire AVG-rechten zijn niet gedocumenteerd in de domein- en solution architectuur. Dit betreft onder andere het recht op inzage, correctie, verwijdering, beperking etc.
- Er wordt geen onderscheid gemaakt tussen gestructureerde en ongestructureerde persoonsdata
- Er is geen gedocumenteerd proces of documentatie aangetroffen die de datakwaliteit van persoonsdata beheerd.
- Er is geen relatie gelegd tussen de strikt te gebruiken persoonsdata en de beschikbare persoonsdata. Er is geen invulling gegeven aan het need to know principe.

Samenvatting bevindingen overig

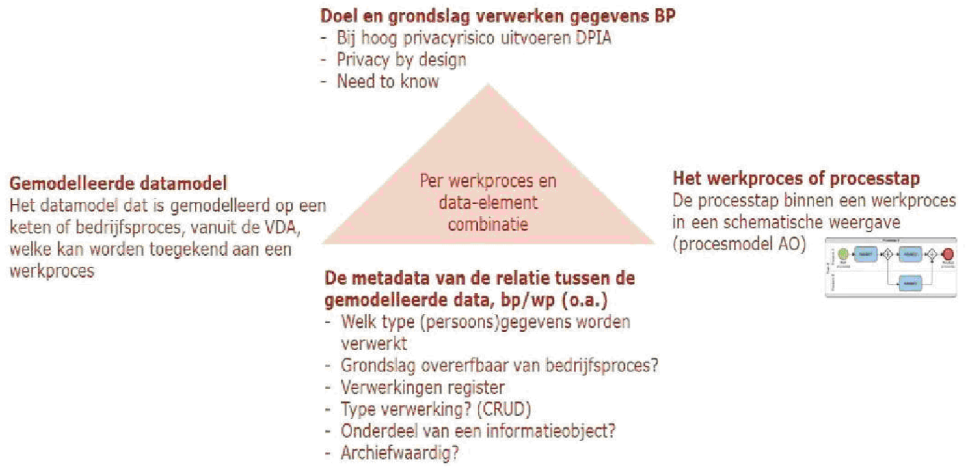


- Er is geen specifiek en concreet beleid op privacy-by-design
- De controlelijst beoordeelt niet integraal de compliantie op AVG, BIO en archiefwet. Het is een deelwaarneming.
- De toepassing van de archiefwet is geen onderdeel van domeinarchitectuur, ook niet van andere ketenprocessen.
- Het wijzigingsproces werkt op onderdelen niet volledig. Een voorbeeld zijn domein architecturen die niet voorzien van een afwijkingsverslag worden afgetekend. In dit afwijkingsverslag staan dan die punten uit de toepasselijke referentiearchitecturen die niet zijn verwerkt in de afgetekende domein architectuur.
- Op nieuwe (2018-2022) applicaties en ontwikkelingen zien we geen wijziging op bovenstaande. Er lopen wel ontwikkelingen maar samenhang en zicht ontbreekt.

4. ‘Samen verbeteren’

Voor verbeteren van het zicht op het verwerken van persoonsgegevens zal de directie Particulieren op ketenniveau een MDT 2.0 inrichten.

Het MDT 2.0 zal langs de lijnen van bestaande toekomstgerichte standaarden (VDA, HDA, kader AO en modelleerconventies procesontwerp) de gegevens en bedrijfsprocessen in één schema modelleren met als doel aantoonbaar compliant te zijn in opzet en bestaan.



Het MDT 2.0 traject duurt zo lang als dat nodig is om deze inzichten voor een bedrijfsproces af te ronden maar kent na 3 maanden wel een evaluatie moment. Het MDT 2.0 zal al lerend producten ontwikkelen en zal zorgen dat inzicht wordt verkregen op benodigde tijd, kennis en expertise, middelen en op het duurzaam in stand houden van de werkwijze.

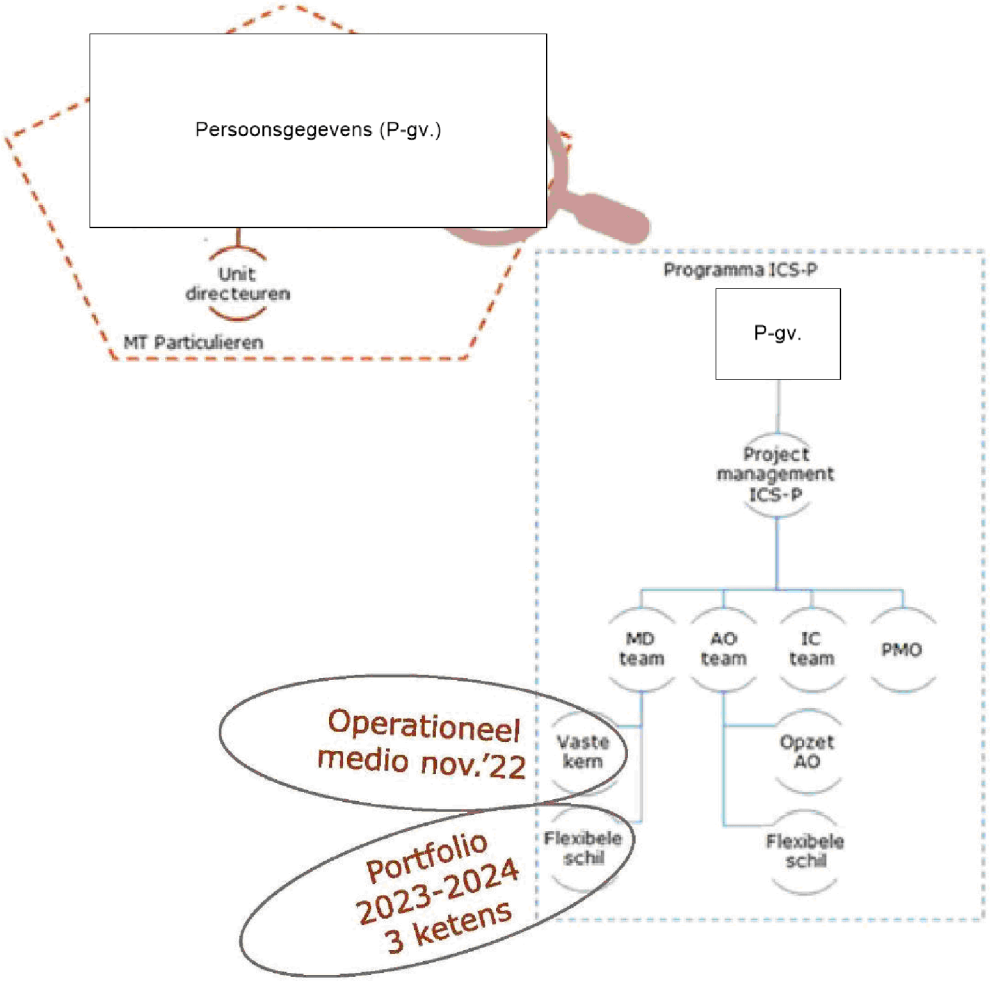
Het streven is per 1 oktober 2023 te starten het uitwerken van casus bij de keten Schenk- en Erfbelasting voor het bedrijfsproces [EB] Afhandelen Aangifte.

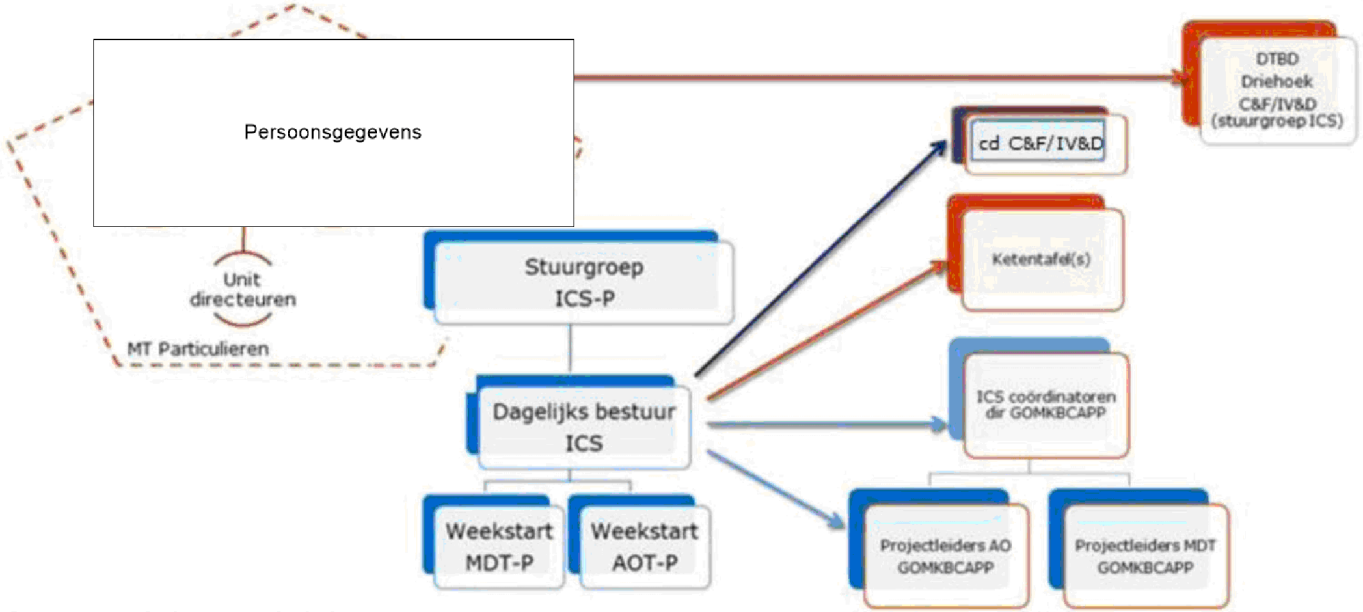
De samenstelling van het MDT 2.0 zal voor het oppakken van deze casus nader en in gezamenlijkheid binnen en buiten de keten bepaald worden, maar bestaan zeker uit leden met operationele kennis van VDA Persoonsgegevens modelleerconventies (AO (Organisatie), procesontwerper IV), de AVG, de archiefwet, Persoonsgegevens van het IDS cluster.

BIJLAGE

AANPAK MDT-P

Organisatie- en overlegstructuur ICS-P





Toepassen controlelijst

Sessie MDT-P met cd IV&D (kadersteller)

- Doel van de controlelijst
- Ontstaan van de controlelijst
- Uitleg gebruik van de controlelijst aan de hand van:
  - ❑ 20211206 Rapport modeluitwerking v1.0_mst
  - ❑ 20211201 Toelichting controlelijst AVG-BIO-Archiefwet v1.1
  - ❑ 20211115 Concept controlelijst AVG-BIO-Archiefwet v0.4
  - ❑ P-gv. ICS 20220909 Bijlage 5. Bedrijfsprocessen toetsen met controlelijst AVG_BIO_AW

Afstemmen vraag ⇔ antwoord

- Kadersteller AVG

P-gv.

- Kadersteller Informatiehuishouding

Instructie architectuur

- Referentie architecten
- Domein architecten

Basis documentatie

Referentie architectuur

- RA Transactie-verwerking
- RA Zaakgericht werken
- RA Gegevenshuishouding
- RA Document en Archiefbeheer
- RA Integrale Beveiliging
- RA Besturing en beheersing
- RA Monitoring (vervangen door RA B&B)
- RA Managementinformatie (vervangen door RA B&B)
- RA Generiek Kantoor

Domein architectuur

- DA Analytics
- DA Gegevens
- DA Generiek kantoor en toezicht
- DA Inkomensheffing
- DA Informatievoorziening
- DA Schenk- en Erfbelasting

Solution architectuur

- Solution architectuur Generiek Document en Archiefbeheer
- Solution Architectuur Generiek Bezwaarproces
- Solution Architectuur UDA Automatisch Bepalen Aangifteplicht
- Solution Architectuur Verbeteren Beheer en Voortbrenging rekenregels
- Solution architectuur Conserverende aanslagen

Documenten

- CGM Inkomensheffing
- CGM Schenk- en Erfbelasting

Interviews, vragen

Inhoudelijke en/of toelichtende vragen toelichtingen opgehaald bij:

- Adviseur Bedrijfsvoering (Vaktechniek)
- Persoonsgegevens
- Business Analisten
- Persoonsgegevens
- Collega's MDT-MKB, GO en CAP
- Datacoördinatoren P
- Domein architecten
- Informatiemanagement IV
- Kadersteller AVG
- Kadersteller Informatiehuishouding
- Persoonsgegevens
- Lead architecten
- Solution architecten
- Product owner
- Persoonsgegevens
- Referentie architecten
- Release Train Engineer
- Persoonsgegevens

Aanvullende documenten

Voor het kunnen beantwoorden van de vragen bleek basis documentatie nog niet voldoende, onder meer de volgende aanvullende documentatie zijn meegenomen bij de toets:

- Jaarplan keten S&E
- Jaarplan keten IH
- Jaarplan keten Gegevens
- Jaarplan directie Particulieren
- Programmarapportage AVG (19 juli 2018)
- AWR, AWB, wet op de inkomstenbelasting, successiewet
- Nieuwsbrieven Toezicht
- Besluiten DTBD (op het terrein van AVG, BIO en AW)
- Waarborgenkader voor selectie instrumenten
- Verwerkingenregister Belastingdienst 2019
- Documenten CP etc.

Afstemmen vraag ⇔ antwoord
- Andere ketens / directies
- Projectmanagement

Afstemmen vraag ⇔ antwoord
- Procesdeskundigen
- Specialisten

Bevindingen controlelijst

Bevindingen controlelijst

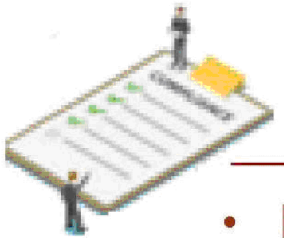
- Controlelijst zelf (niet de invulling ervan)
- Compliantie
- Het MDT
- Toepassen
- Resultaten

Bevindingen AVG

Bevindingen Archiefwet

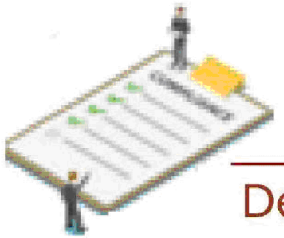
Bevindingen BIO

Bijlage: bevindingen BIO (werking)



De controlelijst zelf (niet de invulling ervan)

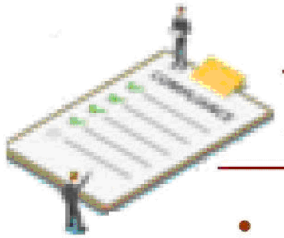
- Er is geen sprake van een volledige compliantie als de controlelijst wordt doorgevoerd.
- De vragen en thema's van de controlelijst kennen een niet benoemd detailniveau.
- De instructie over de toepassing en gebruik van de controlelijst is kort, structuur in de nazorg ontbreekt.
- De controlelijst is of levert geen GEB/DPIA. De controlelijst kan wel de noodzaak daartoe aantonen.



Bevindingen controlelijst: Compliantie

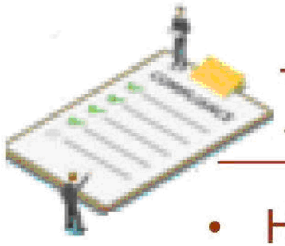
De controlelijst wordt soms ook wel compliantie toets genoemd, maar dat kan de controlelijst niet zijn. Als we de controlelijst zien als een deelverzameling van de drie (AVG, BIO en archiefwet) dan blijkt dat niet alle onderdelen hiervan zijn opgenomen.

Tevens blijkt dat voor elk bedrijfsproces binnen Particulieren, de BIO in de benoemde aspecten nagenoeg beter of scherper wordt "gedekt" door de AVG, en dat tal van hoofdstukken uit de BIO niet worden genoemd in de controlelijst. De BIO zou niet als uitgangspunt voor deze controlelijst hoeven en moeten worden gebruikt.



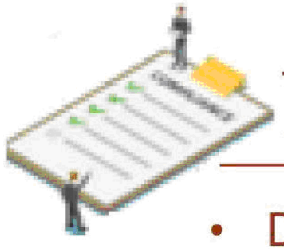
Bevindingen controlelijst: het MDT

- Het MDT-P is een werkwijze die in hoge mate onafhankelijkheid organiseert omdat er geen formele lijnen liggen met andere organisatieonderdelen.
- Kennis van de belastingdienst en het voortbrengingsproces moet worden mee-georganiseerd in het MDT.
- Over het algemeen is er vriendelijkheid en openheid over het onderwerp. Er wordt ruimte gemaakt in agenda's zonder TWR codes vooraf en achteraf. Dit hangt mogelijk af van de aanwezige IV kennis bij het MDT-P.
- Er is initieel uitleg gegeven door de kaderstellers van IV&D, maar daarna tonen ze wel bereidwillig, maar zijn feitelijk weinig betrokken.
- De controlelijst laat zich niet organiseren als een auditplan, waardoor de organisatie van het controlewerk lastig te organiseren is.



Bevindingen controlelijst: toepassing

- Het is aan te bevelen om validatie bij de start in het MDT te organiseren.
- De betrokken medewerkers (van met name het voortbrengingsproces) moeten ook voorgelicht worden over het MDT, de controlelijst en het doel van de controlelijst.
- Een Excel format is niet handig voor het bijhouden van zaken als volledigheid en voortgang. Investeer op zijn minst in een web based tool hiervoor. Deze zijn eenvoudig on-premise te maken.
- De controlelijst heeft een focus op de AVG (9 hoofdstukken) en de Archief wet (1 hoofdstuk).
- De documentatie in de voortbrenging is vaak niet uniform opgezet, wat zorgt voor een langere doorlooptijd.
- De domeinarchitectuur verwerkt niet alle elementen van de dan vigerende referentiearchitectuur.
- De domeinarchitectuur wordt niet aantoonbaar getoetst op compliantie met de toepasselijke referentiearchitecturen.
- De rechtmatigheid (hier komen ze en dit gaan ze doen) van het MDT ontbreekt buiten de directie P, waardoor vragen soms niet of niet volledig beantwoord blijven



Bevindingen controlelijst: resultaten

- Door de vraagstelling in de controlelijst - of in het antwoord op een vraag of als bij aanwezigheid van de documentatie of de organisatie al dan niet is aangetroffen binnen het bepaalde bedrijfsproces - is het bij een negatief antwoord nog steeds onbekend of het een gap is. Door het gebrek aan normen is een negatieve beantwoording van de controlelijst vraag altijd een gap, maar de mate waarin dit een gap is kan niet worden vastgesteld.

- De referentie architectuur wordt beleefd als toekomstmuziek, als een ooit te bereiken status. Vermeldingswaardig is wel dat die toekomstmuziek als het gaat om de AVG, BIO en de archiefwet er maar karig in de DA's vanaf komen.

- In de onderzochte documentatie wordt weinig ingegaan op niet fiscale wet- en regelgeving, de eisen die daarin gesteld worden en de vrijheden die genomen kunnen worden.

Bevindingen AVG

- Er wordt niet of nauwelijks naar de wet (of instructies daarover) verwezen als het al gaat over persoonsgegevens in documentatie
- Persoonsdata wordt niet geclassificeerd als zodanig in documenten als domein- en solution architectuur
- Er wordt geen relatie gelegd tussen werkprocessen en (persoons)gegevens
- Het loggen van elke verwerking van persoonsgegevens is niet aangetroffen in de documentatie. Ook wordt het principe van de GLO niet gedocumenteerd gevonden.
- Het verlenen van toegang tot verwerking van persoonsgegevens is niet gedocumenteerd
- De primaire rechten zijn niet gedocumenteerd in de domein- en solution architectuur, en is geen onderwerp van referentiearchitectuur. Dit betreft onder andere het recht op inzage, correctie, verwijdering, beperking etc.
- Er wordt geen onderscheid gemaakt tussen gestructureerde en ongestructureerde persoonsdata
- Er is geen gedocumenteerd proces of documentatie aangetroffen die de datakwaliteit van persoonsdata beheerd.
- Er is geen relatie gelegd tussen de strikt te gebruiken persoonsdata en de beschikbare persoonsdata. Er wordt dus geen invulling gegeven aan het need to know principe.
- In een enkel geval wordt een solution architectuur voorzien van een WMK toets en een DPIA, maar de GEB-procedure wordt zeker niet geheel gevolgd.

Bevindingen Archiefwet

- De status van de toepassing van de archiefwet is onbekend in de onderzochte processen en documenten
- Er wordt verwezen naar processen of oplossingen die bij IV/CAP of bij CFD bekend zouden moeten zijn, maar niet zijn beschreven in een domeinarchitectuur.
- Op geen van de 11 punten bij het hoofdstuk archiefwet in de controlelijst is een antwoord of een invulling te geven op basis van de huidige (domein en proces-) documentatie en gesprekken.
- Het programma IHH biedt geen inzicht op het onderzochte procesniveau (bijv. ambtshalve aanslag) in de controlelijst
- De aanname dat de controlelijst antwoord kan geven op status van archiefwet op bedrijfsprocesniveau is niet juist.

Bevindingen BIO

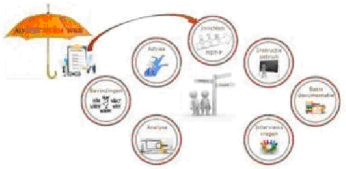
- Het wijzigingsproces werkt op onderdelen niet volledig. Een voorbeeld zijn domein architecturen die niet voorzien van een afwijkingsverslag worden afgetekend. In dit afwijkingsverslag staan dan die punten uit de toepasselijke referentiearchitecturen die niet zijn verwerkt in de afgetekende domein architectuur.
- Als het gaat om zicht op de verwerking en bescherming van persoonsdata komen de beschouwde bedrijfsprocessen er karig van af. Persoonsgegevens worden nauwelijks geclassificeerd als zodanig.
- Er wordt weinig documentatie gevonden van de aan de applicatiecomponent toegewezen applicatiefunctie(s). Dit maakt de samenstelling van de autorisaties niet transparant, en zeker niet als er persoonsgegevens worden verwerkt.
- De BIO aspecten, zoals eerder ook al gemeld, worden beter bediend vanuit de AVG. De BIO met behulp van de controlelijst speelt daarmee geen rol in de beoordeling van de onderzochte bedrijfsprocessen van de ketens vallend onder de verantwoordelijkheid Particulieren.

Aanbevelingen MDT-P

- Neem de geconstateerde omissies over en behandel deze als een bevinding uit een audit. Initieer de oorzaakanalyse, definieer de correctie en corrigerende maatregelen. *(cd IV&D, Keten en IV)*
- Initieer en creëer kaders voor privacy by design. *(cd IV&D, cd vaktechniek)*
- Beëindigen toetsen met de controlelijst en starten met het verbeteren van de omissies met behulp van een control frame work (CFW) voor specifiek de AVG en de archiefwet. De BIO is per definitie een CFW en maak gebruik van de applicatie ITSM. (cd IV&D, cd Vaktechniek, cd C&F)
- Informeer P-gv. over de resultaten van de toetsing door het MDT-P van de onderzochte bedrijfsprocessen. Persoonsgegevens
- Bepaal in hoeverre het programma IHH in staat is om de verplichtingen van de archiefwet na te komen op afzienbare termijn. (SSO CFD, P/BDO/IDS)
- Organiseer de status en de ontwikkeling van niet fiscale wet- en regelgeving in met name de domeinarchitectuur, maar ook in de solution architectuur en het voortbrengingsproces (cd IV&D, cd C&F). Consolideer dit in Privacy-by-design beleid.
- Het team van AVG/BIO en AW specialisten moet aangevuld worden met kennis van IT en in het bijzonder het organisatorische onderdeel van het Belastingdienst voortbrengingsproces. (P-keten en P/BDO/ICS/IDS)

(tussen haakjes de coördinerende verantwoordelijken vanuit het gezichtsveld MDT-P)

Advies voor het traject verbeteren



- Zet een MDT neer op het niveau van de keten voor niet fiscale wet- en regelgeving om zicht te krijgen op het verwerken van gegevens voor de als meest hoog risicovolle geprioriteerde bedrijfsprocessen op het niveau van processtap en activiteit en begin bij de keten S&E voor het bedrijfsproces Afhandelen aangifte erfbelasting.
- Ontwikkel één methodiek/techniek om gegevens én bedrijfsprocessen in één schema gemodelleerd te hebben waarmee compliant beter aantoonbaar is in opzet en bestaan.
- Werk daarbij langs de lijnen van bestaande toekomstgerichte standaarden. (VDA, HDA, kader AO en modelleerconventies procesontwerp) en ontwikkel gaandeweg een werkwijze om het inzicht op te bouwen.
- Het MDT 2.0 duurt zo langs als dat nodig is om deze inzichten voor een bedrijfsproces af te ronden maar kent na 3 maanden wel een evaluatiemoment.
- Bepaal in het MDT 2.0 de benodigde mensen en middelen, complexiteit en het duurzaam in stand houden van de werkwijze.
- Deelnemers zullen nader bepaald worden, maar bestaan zeker uit leden met operationele kennis van VDA Persoonsgegevens modelleerconventies (AO (Organisatie), procesontwerper IV), de AVG én de archiefwet. Betrek ook Persoonsgegevens bij het MDT 2.0.

Bevindingen BIO (werking)

- Bij de directie is voor de getoetste drie bedrijfsprocessen van de ketens niet duidelijk of de beveiligingsmaatregelen doorkomen op operationeel niveau. Zo is een regelmatige (minstens jaarlijkse) communicatie over informatie beveiliging niet aangetroffen (een vereiste zoals opgenomen in de BIO).
- De huidige versie van het Informatiebeveiligingsbeleid is voor het laatst geactualiseerd in 2019 (BIO schrijft een jaarlijkse actualisatie voor).
- Het monitoren en controleren van niet-geautoriseerde toegang wordt door één persoon in de directie Particulieren handmatig en niet gedocumenteerd uitgevoerd. (continuïteitrisico).
- De geïmplementeerde Identity Access Management en Role Based Access procedures zijn niet duidelijk beschreven in de operationele documentatie binnen de LTB procedures.
- De beschikbare operationele documentatie mist duidelijke instructies hoe om te gaan met toekennen en beheren(monitoren) van de rollen.
- Voor de HR procedure: wijziging- of beëindigingsprocedure van het dienstverband is geen uitgevoerde controle (controleerbaar) aangetroffen.
- Het toewijzen en gebruik van speciale toegangsrechten worden binnen de directie buiten de need to know kader toegestaan, er is geen of weinig controle of deze toegang ook weer wordt verwijderd.