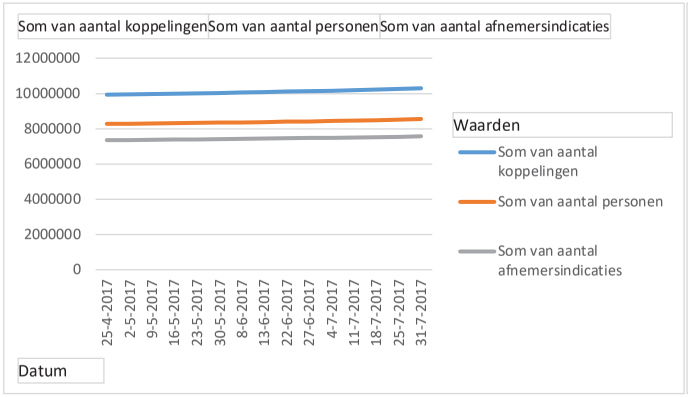
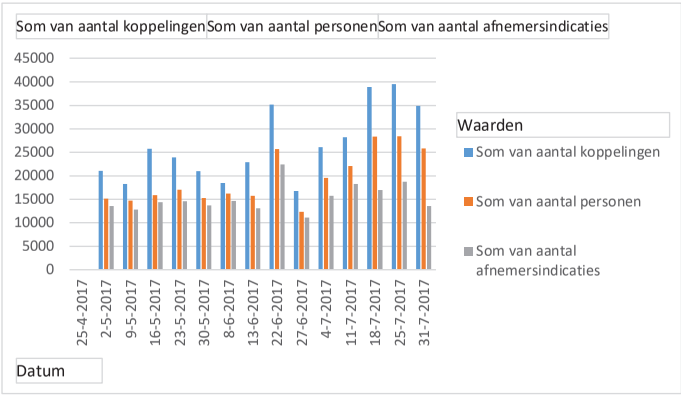
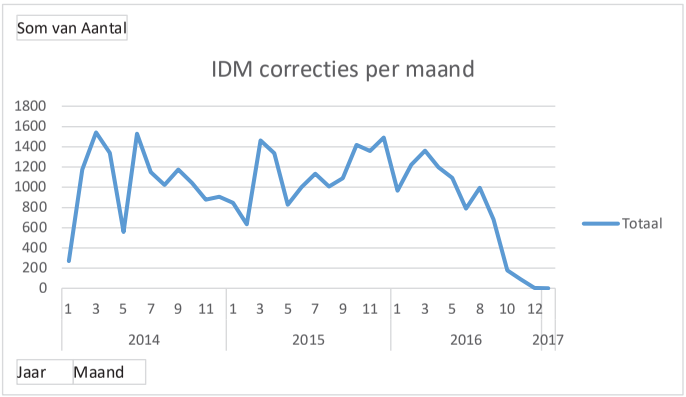
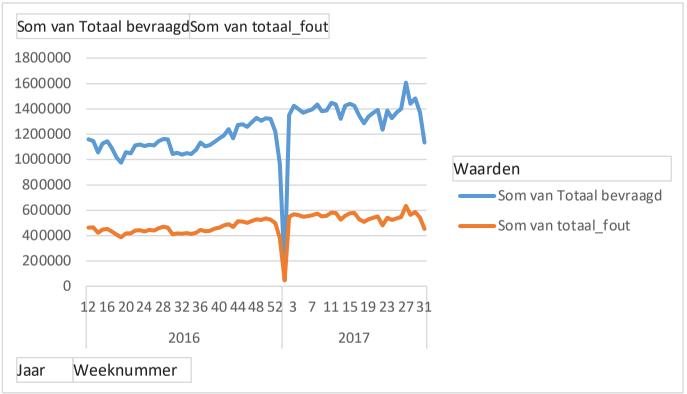
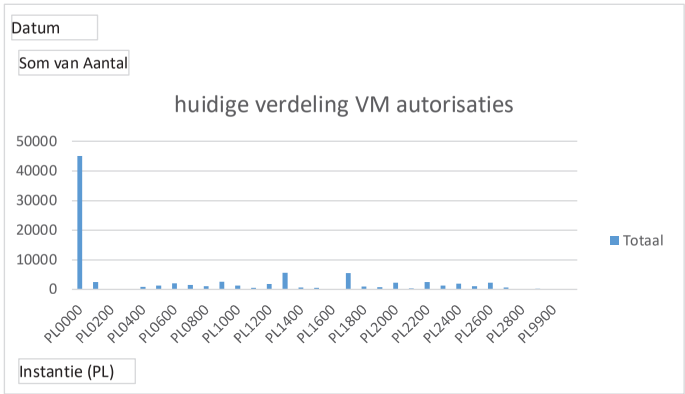
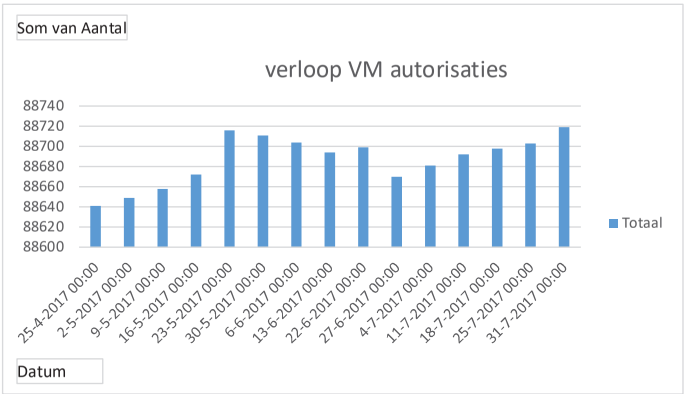

Som van aantal koppelingen
Som van aantal personen
Som van aantal afnemersindicaties
12000000
10000000
8000000
6000000
4000000
2000000
0
25-4-2017
2-5-2017
9-5-2017
16-5-2017
23-5-2017
30-5-2017
8-6-2017
13-6-2017
22-6-2017
27-6-2017
4-7-2017
11-7-2017
18-7-2017
25-7-2017
31-7-2017
Waarden
Som van aantal koppelingen
Som van aantal personen
Som van aantal afnemersindicaties
Datum

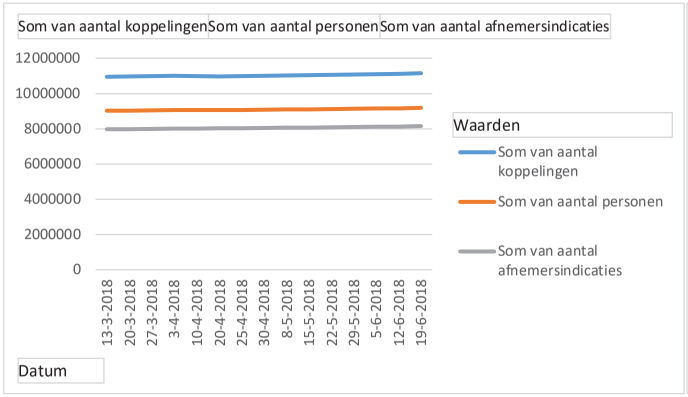

Som van aantal koppelingen
Som van aantal personen
Som van aantal afnemersindicaties
45000
40000
35000
30000
25000
20000
15000
10000
5000
0
25-4-2017
2-5-2017
9-5-2017
16-5-2017
23-5-2017
30-5-2017
8-6-2017
13-6-2017
22-6-2017
27-6-2017
4-7-2017
11-7-2017
18-7-2017
25-7-2017
31-7-2017
Waarden
Som van aantal koppelingen
Som van aantal personen
Som van aantal afnemersindicaties
Datum

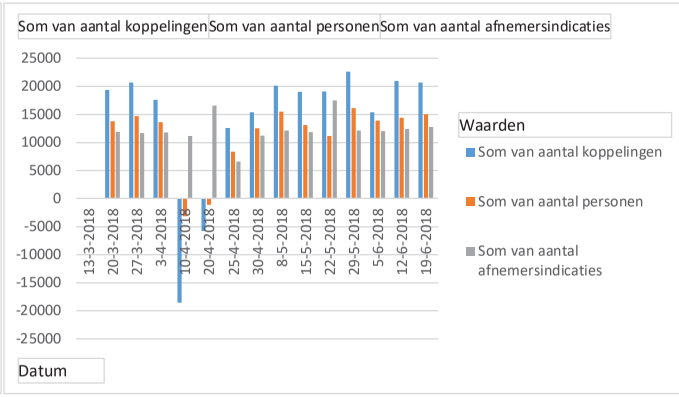

Som van Aantal
IDM correcties per maand
1800
1600
1400
1200
1000
800
600
400
200
0
1 3 5 7 9 11 1 3 5 7 9 11 1 3 5 8 10 12
2014
2015
2016
2017
Totaal
Jaar
Maand

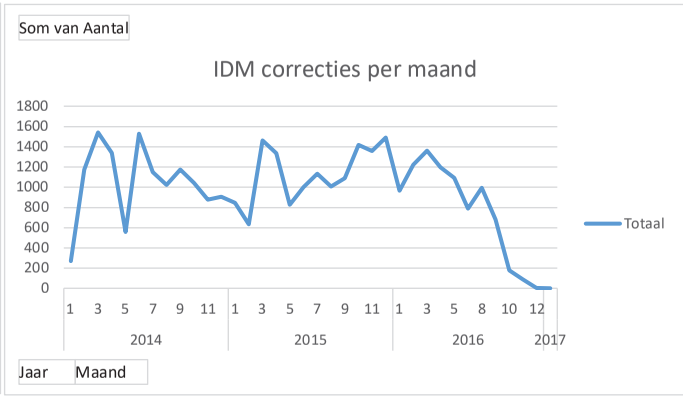

Som van Totaal bevraagd
Som van totaal_fout
1800000
1600000
1400000
1200000
1000000
800000
600000
400000
200000
0
12 16 20 24 28 32 36 40 44 48 52 3 7 11 15 19 23 27 31
2016
2017
Waarden
Som van Totaal bevraagd
Som van totaal_fout
Jaar
Weeknummer

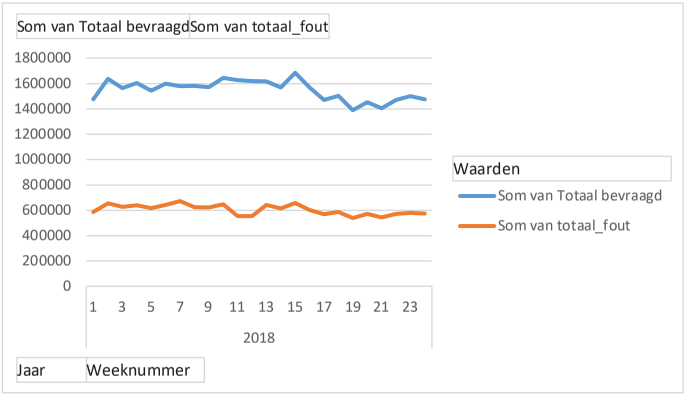

Datum
Som van Aantal
huidige verdeling VM autorisaties
50000
40000
30000
20000
10000
0
PL0000
PL0200
PL0400
PL0600
PL0800
PL1000
PL1200
PL1400
PL1600
PL1800
PL2000
PL2200
PL2400
PL2600
PL2800
PL9900
Totaal
Instantie (PL)

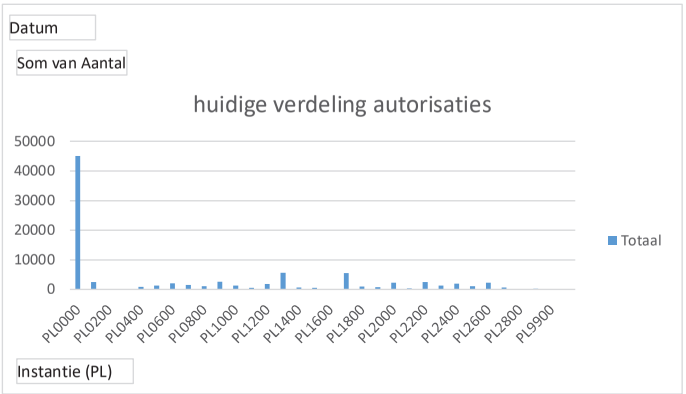

Som van Aantal
verloop VM autorisaties
88740
88720
88700
88680
88660
88640
88620
88600
25-4-2017 00:00
2-5-2017 00:00
9-5-2017 00:00
16-5-2017 00:00
23-5-2017 00:00
30-5-2017 00:00
6-6-2017 00:00
13-6-2017 00:00
22-6-2017 00:00
27-6-2017 00:00
4-7-2017 00:00
11-7-2017 00:00
18-7-2017 00:00
25-7-2017 00:00
31-7-2017 00:00
Totaal
Datum

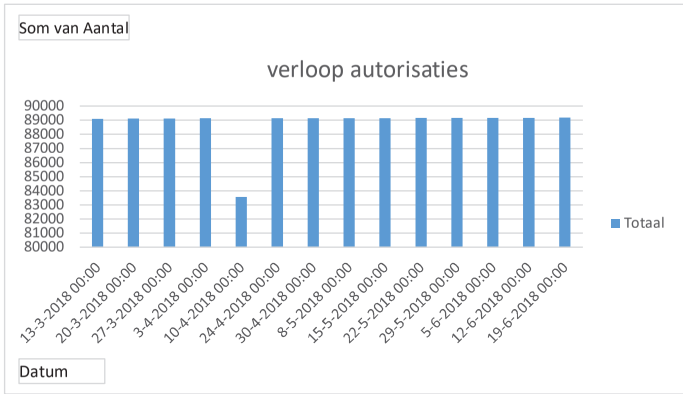

Som van aantal koppelingen
Som van aantal personen
Som van aantal afnemersindicaties
12000000
10000000
8000000
6000000
4000000
2000000
0
13-3-2018
20-3-2018
27-3-2018
3-4-2018
10-4-2018
20-4-2018
25-4-2018
30-4-2018
8-5-2018
15-5-2018
22-5-2018
29-5-2018
5-6-2018
12-6-2018
19-6-2018
Waarden
Som van aantal koppelingen
Som van aantal personen
Som van aantal afnemersindicaties
Datum


Som van aantal koppelingen
Som van aantal personen
Som van aantal afnemersindicaties
25000
20000
15000
10000
5000
0
-5000
-10000
-15000
-20000
-25000
13-3-2018
20-3-2018
27-3-2018
3-4-2018
10-4-2018
20-4-2018
25-4-2018
30-4-2018
8-5-2018
15-5-2018
22-5-2018
29-5-2018
5-6-2018
12-6-2018
19-6-2018
Waarden
Som van aantal koppelingen
Som van aantal personen
Som van aantal afnemersindicaties
Datum


Som van Aantal
IDM correcties per maand
1800
1600
1400
1200
1000
800
600
400
200
0
1 3 5 7 9 11 1 3 5 7 9 11 1 3 5 8 10 12
2014
2015
2016
2017
Totaal
Jaar
Maand


Som van Totaal bevraagd
Som van totaal_fout
1800000
1600000
1400000
1200000
1000000
800000
600000
400000
200000
0
1 3 5 7 9 11 13 15 17 19 21 23
2018
Waarden
Som van Totaal bevraagd
Som van totaal_fout
Jaar
Weeknummer


Datum
Som van Aantal
huidige verdeling autorisaties
50000
40000
30000
20000
10000
0
PL0000
PL0200
PL0400
PL0600
PL0800
PL1000
PL1200
PL1400
PL1600
PL1800
PL2000
PL2200
PL2400
PL2600
PL2800
PL9900
Totaal
Instantie (PL)


Som van Aantal
verloop autorisaties
90000
89000
88000
87000
86000
85000
84000
83000
82000
81000
80000
13-3-2018 00:00
20-3-2018 00:00
27-3-2018 00:00
3-4-2018 00:00
10-4-2018 00:00
24-4-2018 00:00
30-4-2018 00:00
8-5-2018 00:00
15-5-2018 00:00
22-5-2018 00:00
29-5-2018 00:00
5-6-2018 00:00
12-6-2018 00:00
19-6-2018 00:00
Totaal
Datum

Non Functional Requirements BOR

~~ARCHDAT-612~~ - BOR's - Kwaliteitseisen /NFR's DONE

Non-functional requirements (NFR) zijn alle denkbare eisen en wensen die aan een informatiesysteem (website/applicatie, dienst of product), gesteld worden en los staan van wat de gebruiker er allemaal wel of niet mee kan. Meer eenvoudig, functionele eisen zijn direct te relateren aan bedrijfsprocessen en wat het systeem moet doen om dat proces te ondersteunen. niet functionele eisen beschrijven meer hoe het systeem moet werken. Dit zijn vrijwel altijd Systeem Kwaliteit Attributen die de dienstverlening van de software voor ogen heeft.

Goed ingevulde randvoorwaarden maken dat de gebruiker tastbaar profijt heeft van de uitrol van dat ene informatiesysteem. Dit is iets wat we vaak zo goed mogelijk doen, maar weet dat requirement engineering een vakgebied is: https://www.ireb.org/en

Voor alle BasisObjectRegisters (BOR) die op het OPP platform worden gerealiseerd geld dat ze minimaal moeten voldoen aan de gestelde NFR's voor het OPP platform zoals beschreven op: 3.1. Non-functional requirements OPP DIT GAAT WEG.

Non functional requirements, afgeleid ISO_25010 standaarden, zijn te groeperen in productkwaliteit en geschiktheid voor gebruik. In onderstaande tabellen staat het aantal NFR's per onderwerp. Een aantal onderwerpen uit de ISO standaard (geschiktheid voor gebruik) liggen meer op de gebruikers ervaring. Omdat de BOR's meer te beschouwen zijn als een infrastructurele dienst, zijn NFR's voor die groep moeilijker te identificeren.

Non functional requirements die zijn toegevoegd na de laatste review ronde krijgen het label NIEUW tot een nieuwe review is afgerond.

Productkwaliteit	ID	#
Functionele geschiktheid	FUN	9
Prestatie-efficiëntie	PRF	15
Uitwisselbaarheid	UIT	5
Bruikbaarheid	BRUIK	0
Betrouwbaarheid	BET	13
Beveiligbaarheid	BEV	6
Onderhoudbaarheid	OND	10
Overdraagbaarheid	OVD	3

Geschiktheid voor gebruik	ID	#
Effectiviteit	EFF	1
Efficiëntie	EFI	0
Voldoening	VOL	0
Vrijwaring tegen risico	VTR	2
Contextdekking	CON	1

Afhankelijk van het bedrijfsproces / de bedrijfsprocessen waar de dienst voor bestaat is vaak een andere stakeholder onderkent. Per stakeholder zijn NFR's in meer of mindere mate van toepassing.

De BasisObjectRegisters hebben een ondersteunende functie hebben voor vrijwel alle bedrijfsprocessen die we bij de politie onderkennen. Daarom is het lastig om op basis van een bepaald bedrijfsproces, of groepering van bedrijfsprocessen, de NFR's te verzamelen. Onderstaande lijst is dan ook opgemaakt vanuit een algemeen perspectief. Wanneer een BOR ingezet wordt om een bedrijfsproces te ondersteunen, zal er toetsing en aanvulling van de NFR's nodig zijn maar welke een bepaalde prioriteit hebben. Dit past goed in het agile werken waar de Politie voor heeft gekozen.

Voor eenvoudig beheer van de lijst, zie ook bijgevoegd excel bestand: BOR NFR matrix.xlsx

Id#	Groep	Omschrijving	User story	Prio	Vastgesteld op

BOR_NFR_BET_1	Betrouwbaarheid	De BOR's vallen onder het Serviceprofiel Hoog.	Als organisatie hebben we te maken met werkprocessen die dag en nacht, werkdagen en weekend doorgang moeten vinden waarbij onderhoud aan de BOR's zodanig gepland en uitgevoerd moet worden dat ik altijd door kan gaan met mijn werk en gebruik kan blijven maken van de BOR's.		2021-10-01
BOR_NFR_BET_2	Betrouwbaarheid	Het gebruik van CPU en Geheugen mag niet degraderen tijdens normaal gebruik tussen de momenten van gepland onderhoud.	Als organisatie hebben we een bepaalde verwachting van continuïteit in IV dienstverlening, ongeacht het moment van de dag, die ervoor zorgt dat bij tegenvallende resultaten eigen oplossingen worden bedacht buiten het BOR om.		2021-10-01
BOR_NFR_BET_3	Betrouwbaarheid	De BOR's moeten 7 dagen in de week, 24 uur per dag beschikbaar zijn.	Als organisatie hebben we te maken met werkprocessen die dag en nacht, werkdagen en weekend doorgang moeten vinden waarbij onderhoud aan de BOR's zodanig gepland en uitgevoerd moet worden dat ik altijd door kan gaan met mijn werk en gebruik kan blijven maken van de BOR's.		2021-10-01
BOR_NFR_BET_4	Betrouwbaarheid	Verwerken van uniek identificeerbare gegevens mag nooit leiden tot uitgifte van meerdere en verschillende BOR ID's of een conflict opleveren in de uitgifte van een BOR ID.	Als aanroepende applicatie wil ik een identificatie van het BOR ontvangen die verwijst naar een uniek identificeerbaar gegeven zodat ik mijn eigen registratie op eenzelfde manier te verbinden is aan alle overige administraties die over het gegeven gaan.		2021-10-01
BOR_NFR_BET_5	Betrouwbaarheid	De interne afhandeling van gegevensverwerking moet altijd leiden naar een reactie naar de aanroepende partij.	Als aanroepende applicatie wil ik altijd weten dat mijn verzoek is aangekomen en in behandeling is genomen.		2021-10-01
BOR_NFR_BET_6	Betrouwbaarheid	De werking van de BOR's mag niet nadelig worden beinvloed door cyberaanval gerelateerde methoden en technieken als een DDOS en moet blijven voldoen aan de gestelde Prestatie-efficiëntie eisen tijdens normale belasting of momenten van piekbelasting tijdens een dergelijke gebeurtenis.	Als organisatie is het noodzakelijk om om te kunnen gaan met problemen die door derden (DOS aanvallen) worden veroorzaakt zonder verstoring van de dienstverlening		2021-10-01
BOR_NFR_BET_7	Betrouwbaarheid	Een probleem met één applicatieserver mag geen nadelige gevolgen hebben voor de gestelde Prestatie-efficiëntie eisen tijdens normale belasting of momenten van piekbelasting.	Als organisatie is een soepele doorgang van administratie in de huidige tijd te belangrijk om door een serverprobleem te laten verstoren waardoor de dienst moet worden uitgevoerd met voldoende applicatieservers die het werk van elkaar kunnen overnemen als een applicatieserver niet meer werkt.		2021-10-01
BOR_NFR_BET_8	Betrouwbaarheid	Een probleem met de infrastructuur mag geen nadelige gevolgen hebben voor de gestelde Prestatie-efficiëntie eisen tijdens normale belasting of momenten van piekbelasting.	Als organisatie is het noodzakelijk om de BOR's te blijven gebruiken ook al gebeuren er infrastructurele problemen op een locatie waar de applicatieserver werkt en een sdoepele overgang naar een alternatieve locatie moet mogelijk zijn zonder ernstige verstoring van het werk.		2021-10-01
BOR_NFR_BET_9	Betrouwbaarheid	De gegevens die verwerkt worden en verwerkt zijn in de database van BOR's mogen nooit kwijtraken in geval van een fatale fout en altijd direct beschikbaar zijn in een tweede omgeving of instantie die identiek is	Als organisatie is het noodzakelijk om gegevensverwerking altijd doorgang te laten vinden en eenmaal verwerkte gegevens te beschermen voor hergebruik zodat we geen dubbele gegevens gaan verwerken dan wel zaaksgegevens invalideren omdat de BOR's de gegevens niet meer hebben.		2021-10-01
BOR_NFR_BET_10	Betrouwbaarheid	Alle gegevens die door het BOR worden geadministreerd moeten worden backupped, minimaal een keer per week volledig en minimaal elke dag in een incrementele manier.	Als organisatie is het noodzakelijk om alle geadministreerde gegevens veilig te stellen voor catastrofale gebeurtenissen op een consistente en veilige manier zodat gegevensverlies na persistentie minimaal is.		2021-10-01
BOR_NFR_BET_11	Betrouwbaarheid	Alle events die door het BOR verwerkt worden moeten onthouden worden ten minste totdat de volgende incrementele backup succesvol heeft plaatsgevonden zodat gegevens tussen incrementele backups opnieuw uitgevoerd kunnen worden.	Als organisatie is het noodzakelijk dat nooit een succesvolle administratieve handelingen verloren gaat ook al was de backup van de gegevens nog niet geweest.		2021-10-01
BOR_NFR_BET_12	Betrouwbaarheid	Elk jaar word een disaster recovery test gepland en uitgevoerd om zeker te zijn dat herstel van een catastrofale gebeurtenis mogelijk is en dat de stappen om dit proces uit te voeren goed zijn beschreven en regelmatig worden bijgewerkt om de nieuwste technieken voor disaster recovery paraat te hebben.	Als organisatie is het belangrijk om noodprocedures en processen goed en efficient te kunnen uitvoeren en daar ervaring en kennis en kunde in op te bouwen alsook te valideren dat de backup procedures succesvol hebben gewerkt en blijven werken.		2021-10-01
BOR_NFR_BET_13	Betrouwbaarheid	De applicatieve inrichting van de BOR's is opgezen door "machine readable definition files" waarmee de applicatie en infrastructuur opnieuw gecompileerd en opgebouwd kan worden in het geval dat de applicatiecode en inrichting verloren gaat.	Als organisatie hebben we ervoor gekozen om software te bouwen in een agile manier en DevOps in te zetten om de omgeving te beheren waardoor herbouw van de applicatie en applicatieservers vanuit code aansluit bij der gekozen CI/CD aanpak.		2021-10-01

BOR_NFR_BEV_1	Beveiligbaarheid	De BOR's worden periodiek, volgens de richtlijnen van het SOC, onderwerpen aan security audits	Als CIO wil ik dat centraale gegevensvoorzieningen volgens de laatste inzichten beveiligd zijn om persoonlijke en maatschappelijke verstoring te voorkomen die gebeuren bij het verliezen of lekken van gegevens over burgers		2021-10-01
BOR_NFR_BEV_2	Beveiligbaarheid	Toegang tot de BOR's functionaliteiten is bepaald en geregeld via de organisatie brede inrichting en inzet van de autorisatie matrix wat onderdeel is van het Autorisatiemodel Politie	Als gegevens autoriteit wil ik dat alleen geauthentiseerde en geautoriseerde gebruikers met de BOR's kunnen werken om aan de wettelijk bepaalde kaders van de WPG te voldoen.		2021-10-01
BOR_NFR_BEV_3	Beveiligbaarheid	Het verwerken van gegevens in de BOR's voor applicaties en gebruikers buiten het OPP platform, is enkel mogelijk via diensten die door het BOR worden aangeboden, die beveiligd zijn via de in NORA beschreven autorisatie voorkeuren bij gebruik van diensten	Als CIO wil ik gegevens verwerken volgens de wettelijk bepaalde kaders in de WPG en voldoen aan de Nederlandse overheid referentie architectuur		2021-10-01
BOR_NFR_BEV_4	Beveiligbaarheid	Het leggen van een koppeling gebeurd altijd met de verwijzing naar het administratieve gegeven waar de koppeling voor nodig is met alle metadata kenmerken die nodig zijn voor de correcte implementatie van het security model	Als gegevens autoriteit wil ik dat alle gegevens die verwerkt worden in onze organisatie voorzien zijn van gestandaardiseerde en organisatie brede autorisatiekenmerken om oneigenlijk gebruik te voorkomen		2021-10-01
BOR_NFR_BEV_5	Beveiligbaarheid	Het benaderen van gegevens die door een BOR beheerd worden is enkel toegestaan voor aangewezen partijen als de intel	Als CIO wil ik gegevens verwerken volgens de wettelijk bepaalde kaders in de WPG en expliciet aangeven hoe gegevens in onze organisatie verspreid worden voor andere doeleinden		2021-10-01
BOR_NFR_BEV_6	Beveiligbaarheid	De applicatie is bestand tegen de top tien risico's die onderkend zijn bij OWASP	Als CIO wil ik dat bekende problemen in beveiliging uitgesloten worden in de generieke applicaties om aantoonbaar goed bezig te zijn met de informatie voorziening.		2021-10-01
BOR_NFR_BEV_7	Beveiligbaarheid	Het verwerken van gegevens in de BOR's is mogelijk via diensten die door het BOR worden aangeboden die beveiligd zijn via de in de autorisatiematrix beschreven autorisatiekenmerken	Als CIO wil ik gegevens verwerken volgens de wettelijk bepaalde kaders in de WPG en voldoen aan de veiligheidseisen die binnen de organisatie zijn opgesteld rondom het werken met gegevens.		2021-10-01
BOR_NFR_CON_1	Contextdekking	Alle BOR's mogen niet op zichzelf gegevens beheren en vastleggen en zijn altijd gebonden aan een andere administratie waarin het doel van gebruik van gegevens duidelijk aanwezig is.	Als juridische afdeling willen we voldoen aan de WPG voor alle gegevens verwerkingen binnen de politie waarin is bepaald dat zonder een vooraf bepaald doel, deze verwerking niet mag plaatsvinden		2021-10-01
BOR_NFR_EFF_1	Effectiviteit	Een BOR is een algemene dienst voor gelijksoortige gegevensverwerking die ervoor zorgt dat applicaties en bouwers van applicatieis, geen investering in kennisopbouw hoeven te doen voor externe registers, enkel voor het werken met een BOR die voor alle BOR's hetzelfde is.	Als organisatie willen we zo min mogelijk specifieke kennisopbouw hebben die verspreid is over een grote groep ontwikkelaars en gebruikers maar deze kennis centraal organiseren rondom een specifieke extern register		2021-10-01
BOR_NFR_FUN_1	Functionele geschiktheid	Een BOR is enkel beschikbaar om het administratieve proces te ondersteunen en niet uitgebreide onderzoeksvragen te beantwoorden of gegevens in relatie met elkaar te verbinden en presenteren	Als organisatie willen we het administratieve proces en informatieve proces expliciet adresseren in mensen en middelen en de BOR zijn bedoeld om op een eenduidige manier, het beheer en gebruik van de administratieve gegevens die herbruikbaar zijn in functionele en technische zin.		2021-10-01
BOR_NFR_FUN_2	Functionele geschiktheid	Een BOR geeftt toegang tot herbruikbare gegevens van een bekende en vooraf bepaalde kwaliteit	Als organisatie willen we gebruikers nooit laten twijfelen aan de herkomst en correctheid van gegevens die ze in administratieve zin moeten gebruiken. Meningen over de correctheid van de gegevens zullen benaderbaar moeten zijn bij het gebruik van de BOR		2021-10-01
BOR_NFR_FUN_3	Functionele geschiktheid	Een BOR heeft de faciliteiten om meningen terug te koppelen aan het externe register en geeft inzicht wanneer dit heeft plaatsgevonden	Als organisatie willen we gebruikers nooit laten twijfelen aan de herkomst en correctheid van gegevens die ze in administratieve zin moeten gebruiken. Meningen over de correctheid van de gegevens zullen benaderbaar moeten zijn bij het gebruik van de BOR		2021-10-01
BOR_NFR_FUN_4	Functionele geschiktheid	Een BOR heeft de faciliteiten om gebruikers en processen te laten abboneren op mutaties in externe registers en op gebruik van gegevens die reeds geadministreerd zijn of nog geadministreerd worden in het BOR	Als organisatie willen we overeenkomstig met de wettelijke kaders, zo dicht mogelijk bij het gegevensbeheer van een onderwerp, abonnementen administreren zodat we zicht hebben waarvoor en waarop we als organisatie informatie verkrijgen uit externe bronnen via automatische processen		2021-10-01
BOR_NFR_FUN_5	Functionele geschiktheid	Een BOR verlicht het administratieve proces door gegevens uit externe bronnen beschikbaar te maken volgens het semantisch model politie zodat gebruikers op eenzelfde manier met gegevens kunnen werken, ongeacht de applicatie die de BOR gebruikt	Als organisatie streven we zo veel mogelijk uniformiteit van gegevens en gebruiik van gegevens om administratieve processen eenvoudig uitleerbaar te maken met hetzelfde begrippenkader		2021-10-01

BOR_NFR_FUN_6	Functionele geschiktheid	Alle BOR's hebben in in ieder geval dezelfde diensten voor het gebruik van externe registers en het administreren van gebruik van gegevens en abonnementen die worden gezien als CRUD, beheer van relaties en gegevens en abonnementen.	Als organisatie willen we zoveel mogelijk uniformiteit in de diensten die te relateren zijn aan gebruik van registers buiten onze organisatie zodat er een standaard ontwerp voor alle BOR's is wat beheer van de individuele BOR's eenvoudiger en gelijksoortiiger maakt.		2021-10-01
BOR_NFR_FUN_7	Functionele geschiktheid	Een BOR is in staat om gegevens gepagineerd te verstrekken die instelbaar is door de aanroepende partij, zolang deze binnen Prestatie-efficiëntie requirements vallen	Als proces ontwerper en gebruiker wil ik de mogelijkheid hebben om grote lijsten van gegevens op een handzame manier tot me te nemen om te bepalen of mijn zoekkenmerken afdoende waren zonder dat ik langer dan nodig op de resultaten moet wachten dan wel andere gebruikers dwars zit omdat ik alle bandbreedte gebruik		2021-10-01
BOR_NFR_FUN_8	Functionele geschiktheid	Een BOR is in staat om gegevens gesorteerd te verstrekken op basis van meerdere attribuutwaarden die zijn opgegeven door de aanroepende partij, zolang deze binnen Prestatie-efficiëntie requirements vallen.	Als proces ontwerper en gebruiker wil ik de mogelijkheid hebben om gegevens uit een externe bron op een bepaalde volgorde te presenteren zonder daar zelf nieuwe functionaliteiten voor te bouwen		2021-10-01
BOR_NFR_FUN_9	Functionele geschiktheid	Een BOR is in staat om gegevens te filteren voor verstrekking op basis van opgegeven kenmerken over vooraf bepaalde attributen door de aanroepende partij, zolang deze binnen Prestatie-efficiëntie requirements vallen.	Als proces ontwerper en gebruiker wil ik alleen die gegevens uit een externe bron gebruiken die ik nodig heb voor mijn werk.		2021-10-01

5.1.2.i

BOR_NFR_OND_1	Onderhoudbaarheid	Een audit record moet worden bijgeschreven in het audit log (LAAS) voor elke business transactie die wordt uitgevoerd om te voldoen aan logging vereisten	Als organisatie willen we exact weten welke gebruikers bepaalde informatie op een bepaald moment van de dag gebruiken voor hun werkzaamheden zodat we verantwoording van gebruik kunnen afleggen naar samenleving en intern kunnen beoordelen of informatie rechtmatig is gebruikt.		2021-10-01
BOR_NFR_OND_2	Onderhoudbaarheid	Een system record moet worden bijgeschreven in het systeem log voor elke transactie zodat bepaald kan worden of de dienstverlening voldoet aan de gestelde eisen van Prestatie-efficiëntie	Als organisatie willen we inzicht houden hoe goed de dienstverlening is als we deze tegen de non functional requirements aanhouden zodat tijdig beheer van de infrastructuur of inrichting van de software kan plaatsvinden op basis van een planmatige aanpak.		2021-10-01
BOR_NFR_OND_3	Onderhoudbaarheid	Het system log moet analyseerbaar zijn voor beheerders voor ten minste 3 maanden in detail en ten minste voor 3 jaar op dagtotalen.	Als organisatie willen we de non functional eisen rondom schaalbaarheid kunnen analyseren, toetsen en bijstellen op basis van gedetailleerde ervaringscijfers.		2021-10-01
BOR_NFR_OND_4	Onderhoudbaarheid	De diensten moeten gemonitord worden voor alle transacties die buiten het 95e percentiel vallen als deze langer dan 1 minuut duren.	Als organisatie is het van essentieel belang dat de operatie, die een administratief handeling moeten doen, erop kunnen vertrouwen dat er proactief inzicht en beheer plaatsvind wanneer de dienstverlening niet volgens de eisen werkt om situaties te voorkomen waarbij de juiste informatiepositie noodzakelijk is voor goed en juist politiewerk.		2021-10-01
BOR_NFR_OND_5	Onderhoudbaarheid	De hardware waarop de BOR's werken moeten gemonitord worden voor alle transacties om te bepalen dat de beschikbare resources als i/o, cpu niet buiten het 95e percentiel vallen als het gaat om het gebruik van de hardrware	Als organisatie is het van belang om inzicht te hebben wanneer de infrastructuur van centrale dienstverlening tekort schiet om tijdig nieuwe hardware bij te schakelen dan wel preventief beheer te plegen op de bestaande hardware		2021-10-01
BOR_NFR_OND_6	Onderhoudbaarheid	De diensten moeten gemonitord worden dat er geen transacties foutgaan als door onvoorziene situaties.	Als organisatie willen we kunnen ingrijpen om een dienstverlening tijdelijk te staken of aan te passen als blijkt dat er een structurele fout in de uitvoer is ontstaan.		2021-10-01
BOR_NFR_OND_7	Onderhoudbaarheid	De diensten moeten gemonitord worden dat er nooit meer dan vijf transacties achter elkaar foutgaan door een tijdelijke foutsituatie die in een normaal situatie tijdens de uitvoer van de transactie hersteld wordt.	Als organisatie willen we kunnen ingrijpen als er een structureel probleem lijkt te zijn in de dienstverlening aangezien de BOR's een schakel in een langere keten zijn zodat gepaste maatregelen genomen kunnen worden voor ondersteuning dan wel het probleem adequaat op te lossen.		2021-10-01
BOR_NFR_OND_8	Onderhoudbaarheid	De diensten moeten gemonitord worden op gebruik door ongeautoriseerde personen of systemen binnen en buiten de organisatie	Als organisatie willen we kunnen ingrijpen op ongeoorloofd gebruik dan wel patronen in dit soort gebruik te herkennen en onderkennen zodat we onze eigen beveiligingsmaatregelen daarop kunnen afstemmen.		2021-10-01

BOR_NFR_OND_9	Onderhoudbaarheid	De monitoring van diensten moet in staat zijn trends te onderkennen op basis van de afgelopen drie jaar van het Prestatie-efficiëntie, volume en scalability requirements	Als organisatie willen we op basis van vastgelegde gegevens de systemen over een langere tijd kunnen monitoren om requirements bij te kunnen stellen dan wel proactief onderhoud en investeringen doen om te blijven voldoen aan de requirements.		2021-10-01
BOR_NFR_OND_10	Onderhoudbaarheid	De diensten moeten gemonitord worden of alle gelegde koppelingen, in technische, valide zijn om te voldoen aan de WPG.	De koppelingen in het BOR mogen alleen bestaan als er een nut en noodzaak voor is in de vorm van een administratief gegeven dat buiten het BOR wordt beheerd.		2021-10-01
NIEUW BOR_NFR_OND_11	Onderhoudbaarheid	Doorontwikkeling van diensten moet de eerdere versies van dienstverlening ondersteunen om terugwaartse compatibiliteit te garanderen tot de oudere versie niet meer is ondersteund	Als beheerder wil ik mijn diensten met een bepaalde mate van betrouwbaarheid uitleveren aan afnemers en ervoor zorgen dat nieuwe functionaliteiten het koppelvlak van de dienstverlening niet verstoren om afnemers voldoende tijd te geven technische aanpassingen te maken in het koppelvlak.		2021-10-14
NIEUW BOR_NFR_OND_12	Onderhoudbaarheid	Doorontwikkeling van diensten moet in de aansluitvoorwaarden en documentatie zijn beschreven voor alle beschikbare versies van de dienstverlening.	Als beheerder wil ik van alle beschikbare diensten, of ze de laaatste versie zijn of een voorgaande, met duidelijke documentatie kunnen aanbieden aan afnemers.		2021-10-14
NIEUW BOR_NFR_OND_13	Onderhoudbaarheid	Doorontwikkeling van diensten die een nieuwe versie opleveren moet altijd gekoppeld zijn aan een functionele wens, toegespitst naar de verschillende begrippen en taalgebruik van de afnemers van de dienstverlening.	Als beheerder wil ik aan afnemers kunnen uitleggen waarom een nieuwe versie van de dienstverlening is ontstaan en wat de voor of nadelen zijn waar een afnemer mee te maken krijgt in de taal die ze begrijpen.		2021-10-14
NIEUW BOR_NFR_OND_14	Onderhoudbaarheid	Nieuwe versies van diensten moeten expliciet aangeven of het om functionaliteit of om verbetering van veiligheidsacpecten gaat.	Als beheerder van de dienstverlening wil ik voorrang kunnen geven bij de uitrol van nieuwe versies aan alle zaken die met veiligheidsaspecten te maken hebben.		2021-10-14
NIEUW BOR_NFR_OND_15	Onderhoudbaarheid	Benodigde veiligheidsaspecten zijn verplicht voor alle beschikbare versies van dienstverlening	Als beheerder wil ik de veiligheidsaspecten voor alle oude versies veilig kunnen aanbieden.		2021-10-14
NIEUW BOR_NFR_OND_16	Onderhoudbaarheid	Een oude versie van een dienstverlening is voor maximaal één jaar beschikbaar voor afnemers van de dienst	Als beheerder van de dienstverlening wil ik duidelijk zijn hoe lang de ondersteuning van oudere versies van de dienstverlening bestaat zodat het onderhoud zich richt op vernieuwing en verbetering van dienstverlening.		2021-10-14
BOR_NFR_OVD_1	Overdraagbaarheid	Een BOR moet in staat zijn om zonder veel problemen een nieuwe overheidsbron te koppelen als primaire gegevensbron indien dat noodzakelijk i.	Als beheersorganisatie willen we een dienst hebben die eenvoudig aanpasbaar is op de veranderende buitenwereld waar gegevens vandaan komen		2021-10-01
BOR_NFR_OVD_2	Overdraagbaarheid	Een BOR moet modulair zijn gebouwd in de code om zonder problemen verwijderd te worden uit de code wanneer een nieuw pakket of dienst de functionaliteit van het BOR overneemt.	Als organistie willen we aansluiten bij overheidsinitiatieven als een pakket of dienst gekocht moet worden die de diensten van het BOR vervangen en de mogelijkheid open houden om generieke diensten in onze organisatie uit te besteden aan derden indien dit wenselijk en mogelijk is.		2021-10-01
BOR_NFR_OVD_3	Overdraagbaarheid	Het opslagmodel van een BOR moet flexibel en aanpasbaar zijn en het semantisch model politie ondersteunen	Als organisatie willen we voorbereid zijn op wijzigingenm in het semantische model politie zonder uitgebreide herstelwerkzaamheden of delen van de BOR opnieuw te ontwikkelen.		2021-10-01

5.1.2.i

5.1.2.i

BOR_NFR_UIT_1	Uitwissel baarheid	DE BOR's moeten in staat zijn om inpasbaar te zijn in bestaande werkstromen en werkprocessen zoals bekend in onze organisatie voor toekomstige dan wel nog niet geidentificeerde werkstromen en werkprocessen zonder dat de fundamentele aard van het proces hoeft te worden aangepast.	Als organisatie wil ik dat informatie voorzieningen ondersteunend zijn voor gelijksoortig administratief en operationeel werk en gebruik kunnen maken van het generieke karakter van het gegevensbeheer, zonder dat ik mijn werk drastisch hoef aan te passen aan techniek.		2021-10-01
BOR_NFR_UIT_2	Uitwissel baarheid	De BOR's moeten in staat zijn om administratieve processen te ondersteunen met gegevens diensten ongeacht of deze vallen binnen het operationele of bedrijfsvoerings domein met de gepaste beperkingen en kaders die gelden volgens de WPG of AVG.	Als organisatie is het maken van onderscheid in het gebruik van de BOR's voor een bepaald bedrijfsdoel niet wenselijk en zal de inrichting en de autorisatie van gebruik ons moeten helpen om ongeacht het bedrijfsproces, generieke diensten in te kunnen zetten voor eenmalig beheer en meervoudig gebruik van gegevens.		2021-10-01
BOR_NFR_UIT_3	Uitwissel baarheid	De BOR's moeten te gebruiken zijn door andere applicaties die niet perse op het pltform werken waar de technische realisatie van de BOR's heeft plaatsgevonden.	Als organisatie willen we duiding geven waar bepaalde oplossingen gebouwd en beheerd worden, maar niet beperken hoe inzetbaar ze zijn in technische zin zoals beschreven in de NORA referentie https://www.noraonline.nl/wiki/Ontkoppelen_met_diensten		2021-10-01

BOR_NFR_UIT_4	Uitwisselbaarheid	De BOR's moeten in ieder geval benaderbaar en te gebruiken zijn via de openAPI standaarden..	Als organisatie willen we aansluiten bij de door NORA bepaalde paas toe of leg uit standaarden zoals beschreven op https://www.noraonline.nl/wiki/Lijst_Open_Standaarden_voor_Pas_Toe_of_Leg_Uit waar de openAPI standaard als voorkeurstechniek staat benoemd		2021-10-01
BOR_NFR_UIT_5	Uitwisselbaarheid	Alle BOR's gebruiken dezelfde technische vorm voor de aanroep om sortering, filtering en paginering mee te geven.	Als organisatie is het noodzakelijk dat we zoveel mogelijk uniformiteit van code nastreven om een technische taal te spreken bij het technische gebruik van algemene diensten waar de BOR onder valt		2021-10-01
BOR_NFR_VTR_1	Vrijwaring tegen risico	Het gebruik van overheidsregisters is alleen via de BOR's mogelijk zodat we als organisatie in het geheel, grip houden op het gebruik van externe gegevens	Als organisatie wil ik per extern register, maximaal een koppelvlak hebben ingeregeld in technische en functionele zin zodat gebruik van externe gegevens, verantwoording van het gebruik en beheer van het gebruik op een plaats kan gebeuren zodat we veilig, verantwoord en zonder duplicatie van diensten, met externe registers en gegevens kunnen werken.		2021-10-01
BOR_NFR_VTR_2	Vrijwaring tegen risico	Het gebruik van BOR's in een werkstroom of bedrijfsproces is enkel mogelijk na een uitgevoerde gegevens effectbeoordeling en borging van het gebruik in het gegevens register	Als organisatie wil ik per BOR exact weten welke bedrijfsprocessen gebruik maken van de externe gegevens, welke risico's daaraan zijn onderkend en dit borgen in ons verwerkingsregister zodat ik aan auditors kan aantonen zorgvuldig om te gaan met gegevens gebruik en beheer		2021-10-01

Uitwerking architectuur MDM

Op deze pagina vind je de uitwerking van de MDM architectuur.

- Op de pagina patroonkeuze MDM worden de mogelijke patronen in detail beschreven. Dit zijn uitersten. Op deze pagina is de uitwerking waar de politie voor heeft gekozen op basis van een 'best of both worlds' benadering.
- Er ontstaat een stelsel van objectregisters die gezamenlijk de invulling geven aan de MDM ambitie van de politie. Dit vereist samenwerking tussen de (basis-)objectregisters met andere IV componenten. Zie De componenten van het stelsel toegelicht voor de samenhang en een aantal schetsen van use cases hoe de componenten samenwerken.
- Het stelsel zal gefaseerd worden gerealiseerd. Het Overzicht benodigde (B)OR's en roadmap geeft op hoofdlijnen deze fasering en de relatie met het politie portfolio.

Als een uitspraak betrekking heeft op zowel een basisobjectregister als op een objectregister dan wordt dit aangeduid met **(B)OR.** Als er onderscheid bestaat tussen een basisobjectregister (aangeduid als **BOR**) en een objectregister (aangeduid als **OR**) dan is dat expliciet aangegeven.

De MDM architectuur wordt beschreven aan de hand van 'persoon'. Het patroon geldt echter voor alle gegevensobjecten waarvoor een (B)OR wordt gerealiseerd.

Keuzes ten aanzien van MasterData Management - perspectief gegevensarchitectuur

Het stelsel van (basis-)objectregisters maakt onderscheid tussen interne en externe gegevensobjecten

- Een intern gegevensobject is een gegevensobject met gegevens die verwerkt worden in het kader van de uitvoering van de politietaak en die niet afkomstig zijn uit een overheidsregistratie
- Een extern gegevensobject is een gegevensobject met gegevens die verwerkt worden in het kader van de uitvoering van de politietaak en die afkomstig zijn uit een overheidsregistratie

	Extern gegevensobject	**Intern gegevensobject**
Herkomst	Overheidsregistratie	Uitvoering politietaak

Beheerder	Beheerder van de overheidsregistratie	Politie
Gebruik	*as-is.* De politie wijzigt nooit een extern gegevensobject. Geconstateerde fouten worden teruggemeld aan de beheerder.	Actief beheer en gebruik

De kwaliteit van een intern gegevensobject kan verschillen als we kijken naar de mate waarin het intern gegevensobject daadwerkelijk iets zegt over een geïdentificeerd bedrijfsobject. De sortering in onderstaande tabel is van hoog naar laag

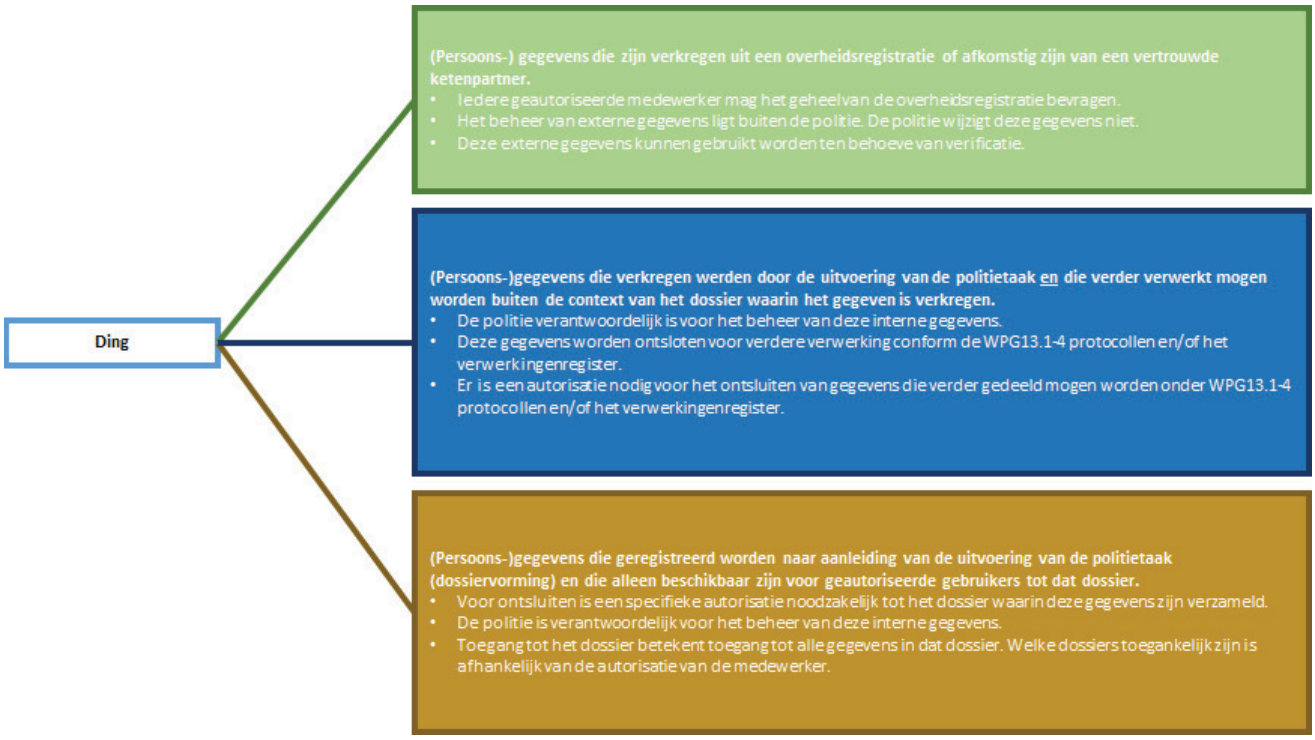
Kwaliteitsaanduiding	**Soort object**	**Toelichting**	**Voorbeeld**
Geverifieerd bij register	Extern gegevensobject	Geverifieerd binnen NL overheidsstelsel(-register). Hoogste kwaliteitsaanduiding, de identiteit was succesvol verifieerbaar bij een overheidsregistratie.	Persoon is geverifieerd bij de BRP.
Opgave van een vertrouwde ketenpartner	Extern gegevensobject	Een vertrouwde ketenpartner geeft de identiteit op waarna de politie deze als waar aanneemt.	Het CJIB geeft naam en adres op bij een executie-opdracht.
Geverifieerd door politie.	Intern gegevensobject	De politie verifieert de identiteit zelf en stelt vast dat de identiteit klopt. De diender moet aangeven op welke manier de identiteit is vastgesteld. Bij het object wordt geregistreerd op welke manier en met welke middelen de authenticatie is gebeurd.	Identiteit van een persoon wordt geverifieerd aan de hand van een identiteitsbewijs. De politie oordeelt dat het identiteitsbewijs echt is en passend is bij het subject.
Ongeverifieerd	Intern gegevensobject	Het gegeven is geregistreerd door de politie en er heeft (nog) geen identificatie plaatsgevonden of de identificatie is mislukt.	Politie treft een wapen aan waarvan de identificerende kenmerken zijn verwijderd. Het wapen wordt wel geregistreerd.

NB

- De herkomst van het gegevensobject bepaal in de context van het stelsel van objectregisters de kwaliteit. Er zijn andere kwaliteitskenmerken, maar die zijn in deze context minder relevant.
- Er zijn meerdere 'beschrijvingen' mogelijk van 'hetzelfde ding in de werkelijkheid'. Bijvoorbeeld dat een persoon zegt A te zijn terwijl na verificatie blijkt dat het toch echt B is. Als intern gegevenobject is dan A vastgelegd en B als extern gegevensobject. De kwaliteit (herkomst) van A is dan 'ongeverifieerd' en van B 'geverifieerd'. Beiden zijn aan elkaar verbonden via het BOR.
- Afhankelijk van het gegevensobject zijn keuzes te maken met betrekking de mogelijke kwaliteitsaanduidingen. Zo zal het BOR dat 'veelplegers' ontsluit alleen de kwaliteitsaanduiding 'geverifieerd bij register' kennen terwijl op bijvoorbeeld een auto of persoon alle vier de kwaliteitsaanduidingen van toepassing zijn.
- Zie ook: Opbouw begrippenkader mbt gebruik gegevens uit overheidsregistraties

De toegang tot gegevens over ‘1 ding in de werkelijkheid’ is beperkt

Niet alle kennis die over '1 ding in de werkelijkheid' bekend is, kan worden hergebruikt. Onderstaande indeling beschrijft de typering van de kennis en de relatie met de autorisatie.



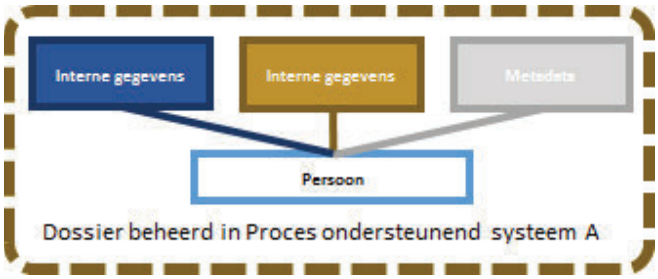
NB

- Deze kleuren worden in de rest van deze architectuur gebruikt.
- Voor een nadere uitwerking van de toepassing van autorisatie, zie de deelarchitectuur autorisatiemanagement.

Een BOR ontsluit kennis over '1 ding in de werkelijkheid' waarvoor verificatie bij een overheidsregister mogelijk is.

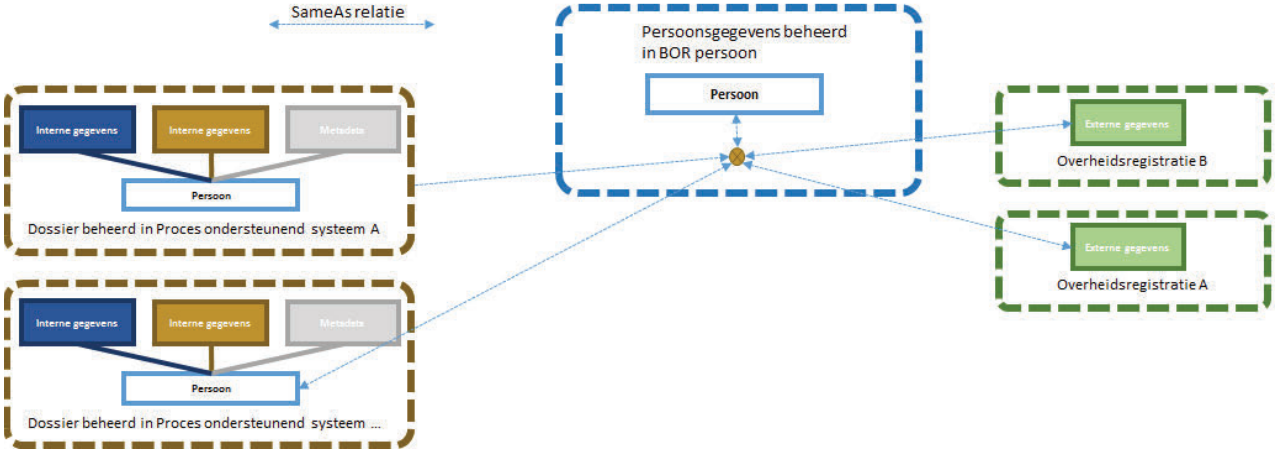
Een BOR verbindt de kennis over '1 ding in de werkelijkheid'. Daarmee verbindt een BOR zowel externe als interne gegevensobjecten; zolang het maar gaat over 'hetzelfde ding in de werkelijkheid'. Het BOR fungeert daarmee als 'sleutelbos' voor POA's, overheidsregistraties en andere (B)OR's. Een BOR beheert deze sleutelbos.

Interne gegevensobjecten worden altijd in een proces ondersteunende systeem geregistreerd. Onderstaande figuur beschrijft dat de kennis over een persoon onder te verdelen is in kennis die beperkt is tot geautoriseerden op het dossier (de 'bruine' gegevens) en en voor gegevens die ook buiten het dossier verder verwerkt mogen worden (de 'blauwe' gegevens).

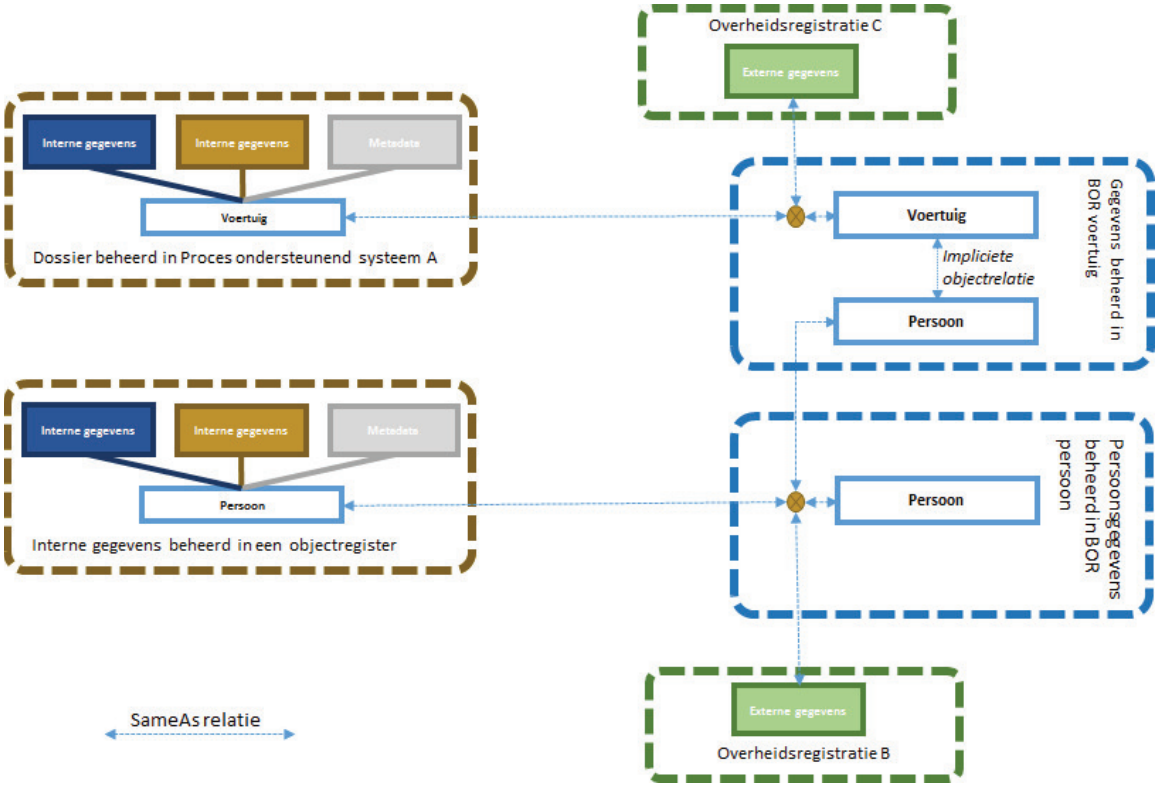


Een BOR beheert geen externe gegevensobjecten (de 'groene' gegevens) maar verwijst er naar. Dit stelt specifieke eisen aan het koppelvlak met de basisregisters. Hoewel de aansluitvoorwaarden en-kwaliteit per overheidsregister verschilt, is het aannemelijk dat de politie zelf invulling moet geven aan een het koppelvlak. De complexiteit van het koppelvlak wordt afgeschermt door het BOR.

Omdat het gaat om kennis over 1 persoon in de werkelijkheid worden de gegevens aan elkaar verbonden middels een same-as relatie. Onderstaande figuur beschrijft de werking van deze relaties. Zoals te zien is worden gegevens over 'hetzelfde ding in de werkelijkheid' verbonden middels same-as relaties via een knooppunt ('sleutelbos') in het BOR. Verder valt op dat het enige gegeven dat in het BOR beheerd wordt deze sleutelbos is. Aangezien de kennis in dit knooppunt niet gedeeld wordt is deze 'bruin'.



Naast proces ondersteunende systemen die bindingen leggen naar deze sleutelbos zijn er ook de andere (B)OR's die deze bindingen leggen. Onderstaande figuur voegt dat toe. Een BOR voert geen beheer over de externe gegevens, maar ontsluit deze slechts en legt de bindingen vast in de sleutelbos.



NB

- Op deze manier ontstaat een samenhangend stelsel van (basis-)objectregisters waarbij gegevens verbonden zijn in plaats van dat er her en der kopieen bestaan.
- *by design* is de kennis over '1 ding in de werkelijkheid' verdeeld over verschillende POA's en (B)OR's. Het combineren van deze kennis tot een actueel en compleet beeld is een taak voor de intel. Zie ook de pragraaf verderop over de relatie met de intel.

Bovenstaande figuren geven aan waar het beheer ligt. Namelijk voor externe gegevens bij de overheidsregistratie. Voor interne gegevens bij een proces ondersteunend systeem of, in het geval van herbruikbare gegevens, bij objectregisters. Dat zegt niet over de functionaliteit van een BOR waarmee de gegevens worden ontsloten. Zoals in onderstaande tabel is te zien, ontsluit een BOR wel degelijk interne objecten.

Kwaliteitsaanduiding	Soort object	Ontsloten via BOR?

Ongeverifieerd	Intern gegevensobject	Nee
Geverifieerd door politie.	Intern gegevensobject	Ja, beperkt tot die gegevenselementen die ook bij een overheidsregistratie beschikbaar zijn.
Opgave van een vertrouwde ketenpartner	Extern gegevensobject	Ja, beperkt tot die gegevenselementen die ook bij een overheidsregistratie beschikbaar zijn.
Geverifieerd bij register	Extern gegevensobject	Ja, volledig.

Het ontsluiten van interne gegevensobjecten die geverifieerd zijn door de politie vereist een toelichting. Het is namelijk de bedoeling dat gegevensobjecten waarvan de politie zelf heeft bepaald wat de identiteit is kunnen worden gebruikt in meerdere dossiers. Als voorbeeld, een buitenlander kan niet worden geverifieerd bij een NL overheidsregister maar kan wel afdoende geïdentificeerd worden met een identiteitsbewijs. Naar deze buitenlander kan dan in meerdere dossiers worden gelinkt.

Bij het ontsluiten van overheidsregistraties geldt het volgende:

- Het is niet wenselijk dat externe gegevensobjecten uit dezelfde overheidsregistratie in meerdere BOR's worden ontsloten. De externe kennis over een bedrijfsobject wordt zo veel als mogelijk ontsloten in 1 BOR.
- Als er meerdere overheidsregistraties zijn die hetzelfde bedrijfsobject beschrijven dan worden die in 1 BOR ontsloten.
- Het BOR combineert deze verschillende overheidsregistraties.
- Er kan maar 1 BOR sleutelbos bestaan voor 1 ding in de werkelijkheid. Als hier administratieve fouten gemaakt zijn dan is er specifieke functionaliteit nodig om te splitsen of samen te voegen.
- We kiezen er voor om de naamgeving van de BOR's conform de 'inhoud' vorm te geven. We kennen dus geen 'BOR Handelsregister' maar een 'BOR Bedrijf'. Zie verder Overzicht benodigde (B)OR's en roadmap
- De politie is niet verantwoordelijk voor het beheer van het externe gegevensobject. Het externe gegevensobject wordt niet aangepast. Het wordt *a s-is* gebruikt.

NB

- Veelal bevat een overheidsregistratie meer kennis over een object dan de politie nodig heeft. We registeren niet meer gegevens dan noodzakelijk. Het is een ontwerpbeslissing welke gegevens we als politie willen ontsluiten, de architectuur legt daar verder geen beperkingen op.
- De exacte indeling van de BOR's wordt in de volgende iteratie gedaan.
- Het is een implementatiekeuze waar de opslag van de herbruikbare interne gegevens gebeurt.
- Er is een autorisatie nodig voor het bevragen van overheidsregistraties. Als deze autorisatie er is dan worden alle achterliggende overheidsregistraties geraadpleegd en deze zijn volledig zonder beperkingen beschikbaar.
- Er zijn nog andere doelen van de politie waarvoor overheidsregistraties van belang zijn. Dit valt met name onder de bronontsluiting in het intell domein en is buiten scope van deze architectuur. Het stelsel van (basis-)objectregisters is namelijk bedoeld voor het verbinden van gegevensobjecten die een rol spelen in dossiers. Bijvoorbeeld door in een dossier aan te kunnen geven waar een incident was en wie daar bij betrokken was. Het gebruiken van complete overheidsregistraties ten behoeve van datamining gebeurt in de intel en leidt niet direct tot het verbinden van de afzonderlijke gegevensobjecten. Dit laatste gebruik valt buiten deze architectuur.
- In ieder geval zal er per basisregistratie (en de daarbij horende sectorale registraties) een koppelvlak ontwikkeld moeten worden.
- Technisch gezien is het de sleutelbos ('kernobject') een intern gegevensobject; als politie voeren we zelf het beheer er over.

Herbruikbare interne gegevensobjecten wordt in een separaat OR ontsloten

Ieder intern, uniek identificeerbaar, gegevensobject wordt op basis van een OR ontsloten. Een OR ontsluit interne gegevensobjecten waarvoor:

- de politie verantwoordelijk is voor het beheer en
- die verkregen worden door de uitvoering van de politie taak en
- meervoudig gebuikt kunnen worden in een zaak of tussen zaken.

Overwegingen bij het bepalen of een bepaald gegevensobjecttype in een dossier of in een OR ontsloten wordt. Een OR is aan te bevelen als het gegeven:

- Beschikbaar stellen voor hergebruik van gegevens onder Wpg art. 13 is voor algemeen politiewerk. Hiervoor bestaan per protocol bewaar en schoningsregels.
- Nuttig is voor meerdere procesondersteunende systemen en/of dossiers.
- Relatief stabiel is in de tijd.
- Exclusief bij 1 object hoort.
- Context onafhankelijk is qua betekenis.

NB

- het is aan de materiedeskundigen om per gegevenselement deze afweging te maken. De architectuur legt niet op voorhand een beperking.
- Een OR wordt altijd bevraagd op basis van een autorisatie. Het resultaat van een bevraging kan daarom 'in rijen' beperkt worden op grond van een autorisatie. Ook kan een bevraging een beperking 'in kolommen' hebben als het resultaat alleen gedeeld mag worden op basis van hit-nohit.
- Interne gegevensobjecten die beheerd worden in een OR kunnen bestaan zonder een verwijzing naar het BOR.
- Zie ook: Opbouw begrippenkader mbt gebruik gegevens uit overheidsregistraties

Voor nieuwe proces ondersteunende systemen is er geen andere manier om herbruikbare gegevensobjecten te ontsluiten dan via een (B)OR

Het stelsel van objectregisters is bedoelt voor alle registratieve systemen. Het is een voorschrift om een (B)OR te gebruiken in iedere nieuw procesondersteunend systeem,

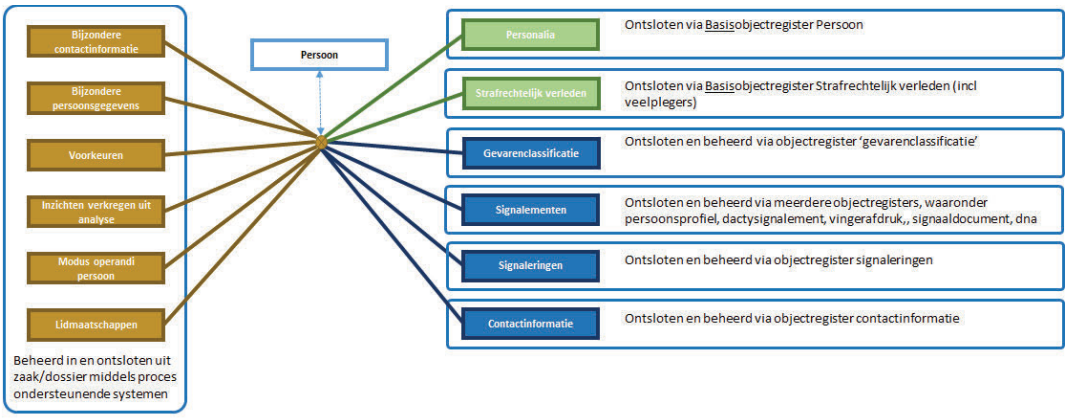
- Een nieuw proces ondersteunend systeem zal externe gegevensobjecten betrekken vanuit een BOR.
- Voor nieuwe proces ondersteunende systemen die interne gegevensobjecten willen ontsluiten is er geen andere manier dan via een OR.

NB

- De (B)OR's zullen de aankomende jaren gefaseerd beschikbaar komen.
- Ontwikkelingen in nieuwe procesondersteunende systemen, vooruitlopend op de realisatie van de (B)OR's, zullen in hun architectuur rekening moeten houden met de aansluiting op het stelsel.

De kennis over '1 persoon in de werkelijkheid' is verdeeld over meerdere systemen

Onderstaande figuur laat zien dat de kennis over '1 persoon in de werkelijkheid' *by design* is verdeeld over proces ondersteunende systemen en (basis-) objectregisters. Deze gedistribueerde kennis is combineerbaar omdat overal verwezen wordt naar 'dezelfde persoon in de werkelijkheid'.



NB bovenstaande is ter illustratie
- De exacte indeling en naamgeving van de (basis-)objectregisters wordt nog bepaald.
- Niet alle (basis-)objectregisters zijn opgenomen.

NB

- Het bevragen en combineren van alle kennis is een taak voor de intel.
- In het verleden werd zo'n gecombineerde bevraging ook wel een kernregister genoemd. Om verwarring te voorkomen wordt deze term niet meer gebruikt.

Gegevens in een (B)OR worden niet veranderd, er worden aanvullende uitspraken gedaan ('append only')

Alle gegevens die de politie beheert worden in beginsel niet gecorrigeerd door het overschrijven maar door het doen van een nieuwe uitspraak en het beeindingen van de vorige. Dat betekent dat iedere uitspraak die de politie registreerd, wordt voorzien van metadata aan de hand waarvan de geldigheid (op een bepaald moment) kan worden bepaald.

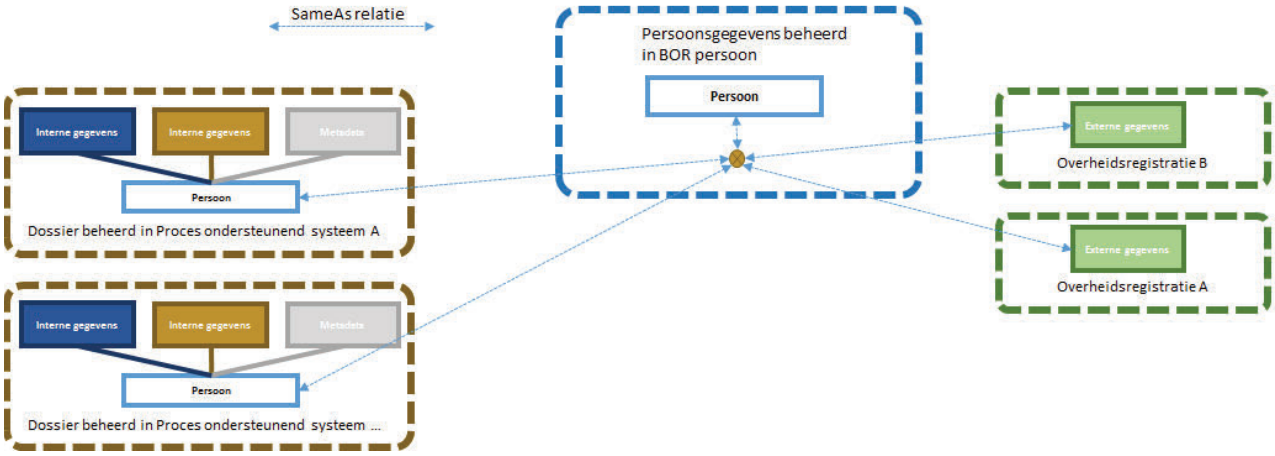
Op een willekeurig moment kunnen er meerdere uitspraken gedaan zijn die over hetzelfde gaan. Bijvoorbeeld uit de BRP blijkt dat een persoon woont op adres A terwijl de politie contstateerd dat deze persoon op B woont. Hoewel beide uispraken niet tegelijkertijd gedaan worden, kunnen ze beide wel tegelijkertijd geldig zijn. Bij het bevragen van het stelsel van objectregisters moet dus steeds rekening gehouden worden met de geldigheid van een uitspraak en de mogelijkheid dat er meerdere uitspraken zijn die elkaar kunnen tegenspreken. In de UX moet hier rekening mee gehouden worden. Het is aannemelijk dat de weergave/dialoog in de UI wordt beinvloed door de specifieke handeling en bevoegdheid van de gebruiker.

NB

- De externe gegevensobjecten worden ontsloten *as-is*. Als we als politie aanvullende uitspraken willen doen, dan leidt dat tot een intern gegevensobject dat verbonden is aan 'hetzelfde ding in de werkelijkheid'.
- Bij het bevragen van het (B)OR worden standaard de meest recente gegevens geretourneerd met herkomstinformatie.
- Op deze manier is het altijd mogelijk om een bepaalde stand in de tijd samen te stellen en in de UI conflicterende uitspraken weer te geven.
- De functionaliteit van het BOR moet het mogelijk maken om tijdsafhankelijk te bevragen.
- De intel zal ook rekening moeten houden met het tijdsafhankelijk bevragen.
- Van ieder gegevensobject is de herkomst bekend. Het is van belang dat de gebruiker weet wat de herkomst is zodat de herbruikbaarheid bepaald kan worden in relatie tot de politietaak. In de UX moet duidelijk zijn bij de weergaven van het object wat de herkomst is. Bv een groen vinkje bij het object als het gegeven uit een overheidsregistratie komt.

Een BOR verbindt meerdere administratieve perspectieven op '1 ding in de werkelijkheid'. Dat 'ding' duiden we technisch aan middels een URI (=unieke politie sleutel).

Er zullen altijd meerdere administraties zijn die over hetzelfde ding gaan, zowel binnen als buiten de politie. Voor een persoon is dat bv de BVV, SKDB en GBA maar ook de politie eigen applicaties als RAPP. Overal waar we willen verwijzen naar hetzelfde ding in de werkelijkheid gebruiken we de URI van de 'sleutelbos'. In onderstaande figuur is het bolletje vanaf waar alle relaties liggen de 'sleutelbos'. Deze heeft een uniek en stabiel 'adres' in de vorm van een URI.



NB

- Een URI is bedoeld voor technische verwijzingen. De 'vorm' van een URI is niet geschikt voor eindgebruikers.
- Een 'publieksvriendelijk nummer' wordt als extra label aan een object gegeven en in de communicatie gebruikt.
- Legacy applicaties kunnen niet overweg met URI's, deze aanvullende publieksvriendelijke nummers zullen voor legacy applicaties gelden.
- Als een overheidsregistratie URI's uitgeeft voor de door haar beheerde gegevensobjecten dan wordt deze kennis ook met same-as relatie gelegd. Een (B)OR en POA gebruikt voor de verwijzingen onderling uitsluitend door de politie gemunte URI's.
- Zie Relatie met andere architectuurkaders en beleid, hier staat een overzicht van voorschriften met betrekking tot het vormgeven van de URI.

Zoeken in een (B)OR levert de URI van de 'sleutelbos' inclusief gegevens

Het zoekresultaat bevat bij unieke identificatie:

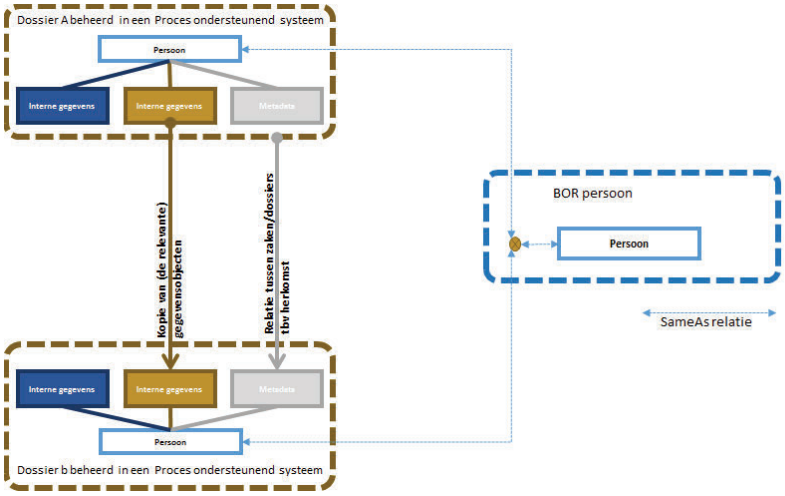
- De URI van de 'sleutelbos', deze dient gebruikt te worden voor de duurzame verwijzing naar het (B)OR.
- Voor een BOR:
    - Een samenvatting van de 'sleutels' van de externe bronnen. Dit zijn in ieder geval de functionele sleutels (bv BRN, SKDB-nummer, V-nummer, etc). Als de overheidsregistratie zelf ook URI's heeft uitgegeven, dan zijn deze ook onderdeel van het zoekresultaat.
    - Het bevragen van een BOR levert de combinatie van interne en externe gegevensobjecten.
    - Voor interne gegevensobjecten geldt dat de kwaliteit voldoende moet zijn (zie de paragraaf hier over).
    - De resultaatset wordt 'in kolommen' beperkt tot die gegevenselementen die via een overheidsregister ontsloten kunnen worden.
- Voor een OR
    - Een samenvatting van de 'sleutels' van de interne bronnen. Dit zijn in ieder geval de functionele sleutels en de URI's.
    - Het zoekresultaat kan worden beperkt omdat per bevraging de autorisatie van de gebruiker wordt meegewogen.
- De dataset wordt conform SMP opgebouwd.
- Wil je meer weten dan de geretourneerde resultaatset, bijvoorbeeld omdat er meerdere (B)OR's of POA's gecombineerd moeten worden, dan leidt tot een bevraging van de intel.

Hergebruiken van interne gegevensobjecten onder beheer van een procesondersteunend systeem gaat middels kopie in combinatie met het opslaan van herkomstinformatie.

De interne gegevensobjecten die worden beheerd vanuit een POA en waarvoor dossier specifieke autorisatie geldt (de 'bruine' gegevens) kunnen alleen via een kopie worden hergebruikt in een vervolgdossier. Op deze manier wordt voorkomen dat autorisatiecomplexiteit tussen dossiers gedeeld moet worden.

Interne gegevensobjecten die op grond van hun autorisatiekenmerken verder verwerkt mogen worden hoeven niet gekopieerd te worden.

Zoals hierboven is uitgewerkt, zal het bevragen van een BOR alleen die gegevenselementen opleveren die ook beschikbaar zijn in een overheidsregistratie. Alle aanvullende kennis (die dus in andere gegevenselementen wordt geregistreerd) is te ontsluiten vanaf het dossier. Het is een implementatiekeuze hoe dit ingevuld gaat worden. Op logisch niveau (dwz het niveau van uitwerken van deze architectuur) doen we geen uitspraken.



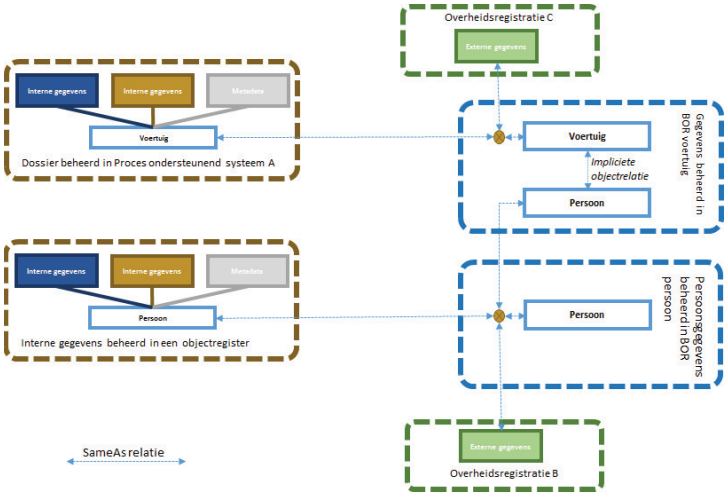
NB

- Het is een functionele keuze of alle gegevens worden gekopieerd of een deel.
- In de volgende iteratie zal de implementatie van het hergebruiken van dossiergebonden ('bruine' gegevens) worden uitgewerkt.
- In de UX moet duidelijk worden vanaf welke zaak de kopieractie gestart moet worden.
- Welke zaken als 'bron' kunnen dienen is afhankelijk de bevoegdheden van de gebruiker. Het identificeren van de relevante en toegankelijke zaken is geen functionaliteit van het BOR maar van de applicatie/intell.
- De gekopieerde gegevenselementen worden in het dossier opgenomen, welke op zijn beurt weer verbonden kan zijn middels een 'sameas relatie' met het BOR .
- Bij het vervolgdossier wordt herkomstinformatie (metadata) vastgelegd.

Impliciete objectrelaties worden expliciet opgeslagen

Bij het bevragen van overheidsregistraties worden in een aantal gevallen verwijzingen naar gerelateerde gegevensobjecten verkregen. Zo kent het handelsregister (HR) de verwijzingen naar de eigenaren (natuurlijke personen). Deze relatie wordt een impliciete objectrelatie genoemd. Als het relevant is voor de politie om deze impliciete relaties op te slaan, dan wordt dat als volgt ingevuld:

- De impliciete objectrelatie wordt in het BOR ontsloten. Dus de relatie tussen een onderneming en een persoon (bestuurder) hoort bij het BOR-bedrijf. Deze relatie mag als authentiek worden gezien. De gegevens over de bestuurder niet.
- Als er functionele noodzaak is, wordt de URI voor de gerelateerde persoon opgezocht in het BOR-persoon.
- Het BOR persoon initieert verificatie.
- De binding tussen het BOR-Bedrijf en BOR-persoon wordt gelegd als de verifcatie is gelukt.
- Als de verificatie van de persoon niet is gelukt wordt er een nieuwe URI gemunt voor deze persoon en de gegevens worden opgeslagen met de kwaliteitsaanduideing 'Opgave van een vertrouwde ketenpartner'.



NB

- Per overheidsregistratie moet beoordeeld worden welk gegeven authentiek is. Bij het HR zijn bepaalde gegevens authentiek en andere gegevens niet. Zo is de link tussen een natuurlijk persoon en een onderneming authentiek, maar de nationaliteit van een natuurlijk persoon is weer NIET authentiek. Met andere woorden: je kunt er wel zeker van zijn dat het gegevenselement "persoon is eigenaar van onderneming" klopt, maar je kunt er niet zeker van zijn dat het gegevenselement "persoon heeft nationaliteit" klopt in het HR. Die bron is dus minder betrouwbaar als de bron in het BRP.

Het conceptuele, logische en uitwisselingsmodel van het BOR is gedefinieerd in het semantisch model politie (SMP)

Het gegevensmodel (MIM1 t/m 3) voor de BOR's is volledig gedefinieerd in het SMP. Dat gaat over zowel de inhoudelijke kennis over het object als alle relevante metadata.

Uitwisselingsmodellen zijn volledig beschreven in het SMP als een semantisch interactiemodel. Dit geldt voor:

- De interface tussen de koppelvlakvoorzieningen en de BOR's.
- Alle op het BOR aangesloten applicaties (met uitzondering van OPP als het BOR wordt geïmplementeerd op OPP).
- Het publiceren van de wijzigingen en bindingen in een (B)OR.

NB de constructie en toepassing van het SMP is uitgebreid beschreven op confluence.

Het BOR bevat twee verwijsindexen; een voor de externe verwijzing naar de overheidsregistraties en e en voor de politie-systemen.

- De externe verwijsindex bevat de verwijzende sleutels naar de overheidsregistraties en de URI die de politie zelf heeft gemunt. Hoe de verwijzing er uit ziet zal sterk afhangen van de eigenschappen van de overheidsregistratie.
- De interne verwijsindex is gericht op het opslaan van de kennis mbt het hergebruik ('in welk dossier/zaak wordt het object gebruikt?'). Deze verwijsindex bevat de URI van het BOR-object en de URI van de betrokken registratie. Deze verwijsindex wordt uitsluitend gebruikt door het BOR om te weten wanneer er geen gebruik meer wordt gemaakt door de registraties van het betreffende object en deze verwijderd kan worden. In de figuren in deze architectuur is deze 'sleutelbos' daarom weergegeven met een bruine kleur.

De 'reden van wetenschap' wordt niet gedeeld bij het bevragen van het BOR

- Het BOR heeft alleen de verwijzingen naar de zaken/dossiers inclusief het systeem dat het dossier beheert. Daarmee heeft het BOR impliciet de 'reden van wetenschap' over waarom we het gegeven überhaupt hebben. Door het bekijken van de bindingen kan namelijk bepaald worden waarom we een bepaald BOR-object hebben.
- Deze kennis is niet vrij te delen. Als we bv een persoon in het BOR hebben omdat deze in een art9 geclassificeerde zaak een rol speelt, dan is deze kennis over de binding beperkt tot de collega's die daartoe een bevoegdheid hebben.
- Het BOR deelt nooit de reden van wetenschap, maar legt uitsluitend de binding ten behoeve van het life cycle management.
- Als een collega wil weten waarom we een bepaald object kennen, dan wordt deze vraag beantwoord door het bevragen van de dossiers (via intel) waar de autorisatieregels worden toegepast..
- Ter illustratie: een gebruiker met rechten op art 8 zoekt een persoon maar krijgt geen deze niet te zien. Vervolgens legt hij deze persoon vast met voldoende identificerende kenmerken, waardoor hergebruik mogelijk is. Het systeem legt dan weldegelijk de same-as relatie.

De interne verwijsindex wordt uitsluitend gebruikt voor het uitvoeren van het life cycle management

- Het initiatief voor het doorhalen van de binding bij het BOR ligt bij het beherende dossier.
- Op het moment dat het dossier wordt vernietigd wordt ook de binding bij het BOR vernietigd.
- Bij het verdwijnen van de laatste binding ('regel in de interne verwijsindex') kunnen alle gegevens in het BOR verwijderd worden. Hier geldt het principe 'geen binding betekent geen noodzaak voor het handhaven van het BOR-object'.
- NB het verwijderen en/of het veranderen van de autorisatiekenmerken heeft geen invloed.

Abonnementen

Uitgangspunten:

- Een abonnement wordt door een basisobjectregister bij een overheidsregistratie afgesloten, bijvoorbeeld door een afnemerindicatie te plaatsen. Wijzigingen in een overheidsregistratie worden middels een notificatie verzonden.
- Het Dossier bepaalt of een abonnement bij een overheidsregistratie gewenst is. Het BOR bewaart deze indicatie en zorgt voor het abonneren bij de betreffende overheidsregistratie(-s).

Abonnementen en notificeren wordt ook door blueview4 verzorgt.

Keuzes ten aanzien van MasterData Management - perspectief autorisatie

Iedereen met een geldige autorisatierol mag de identiteit van een bedrijfsobject vaststellen.

Bij de identiteitsvaststelling van een bedrijfsobject waarvan de gegevens vanuit een BOR ontsloten worden geldt dat iedere medewerker met een geldige autorisatierol de betrokken overheidsregisters in volledigheid mag raadplegen.

Bijvoorbeeld: iedereen met de autorisatierol 'medewerker dagelijkse politietaak' mag het BRP raadplegen om de identiteit vast te stellen van een persoon.

Of de te identificeren persoon al een eerdere relatie heeft bij een andere politie-registratie had, maakt daarbij niet uit.

Zodra de identiteit is vastgesteld, voert het BOR 1 van de onderstaande functies uit:

- Het object is voor het eerst geïdentificeerd (met andere woorden, het is nieuw voor de politie):
  - het gegevensobject wordt in het BOR aangemaakt,
  - een URI wordt gemunt
  - de binding wordt gelegd.

- Het object heeft al een bestaande binding:
  - Een extra binding wordt toegevoegd.
  - Het object wordt geactualiseerd.
  - Wijzigingen worden gepubliceerd (zie ook de paragraaf over abonnementen)

Voor verwerking van de interne gegevensobjecten gelden de autorisatieregels van het dossier

Aanvullende gegevens over 'hetzelfde ding in de werkelijkheid' blijven bij de zaak en kunnen alleen gedeeld worden op grond van de specifieke bevoegdheden die gelden voor die zaak.

Keuzes ten aanzien van MasterData Management - perspectief applicatie-architectuur

Nieuwe proces ondersteunende systemen maken gebruik van het stelsel van (basis-)objectregisters

Nieuwe zaaksystemen zijn die toepassingen die op basis van de volgende platformen/architecturen ontwikkeld worden ter ondersteuning van de taakstelling van de operatien:

- OPP (waaronder RAPP)
- MASA
- Low-code
- GI/HAAS

NB

- De (B)ORS komen gefaseerd beschikbaar. Bij het ontwikkelen van de architectuur voor deze platformen moet rekening gehouden worden met de migratie naar het stelsel.

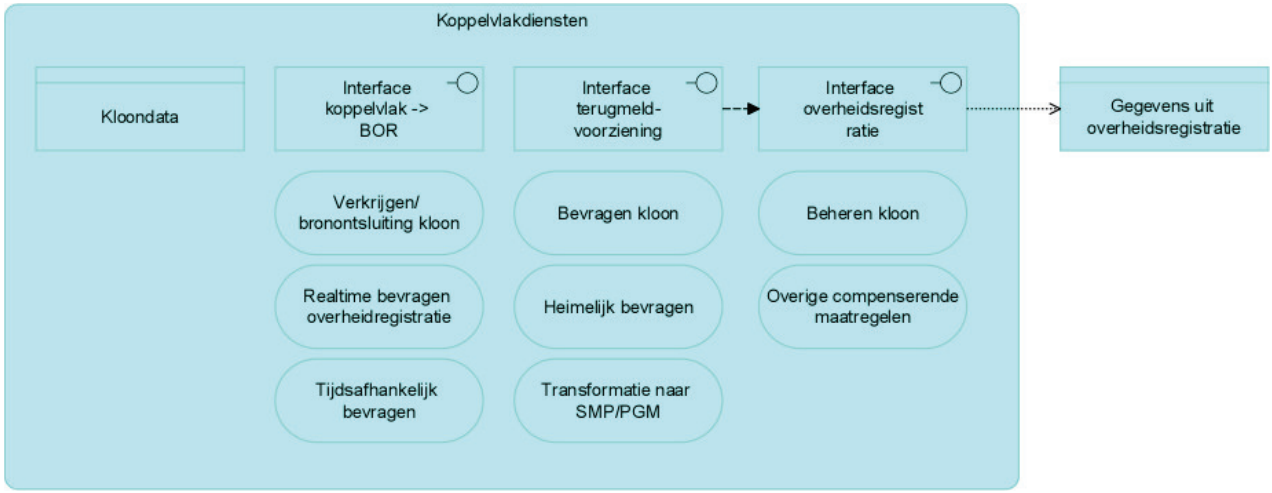
Een (B)OR heeft geen UI voor eindgebruikers

Er zal wel functionaliteit ontwikkeld worden, onder andere ten behoeve van:

- Splitsen en samenvoegen van gegevensobjecten.
- Beheren van abonnementen en het ondersteunen van het notificatieproces.
- Beheren van referentiestandaarden.

Het koppelvlak naar de overheidsregistraties is geen onderdeel van de BOR functionaliteit maar is rand voorwaardelijk voor het functioneren van een BOR.

Onderstaand schema beschrijft de gegevens, interfaces en diensten die per koppelvlak naar een overheidsregistratie noodzakelijk zijn om een BOR te laten functioneren.



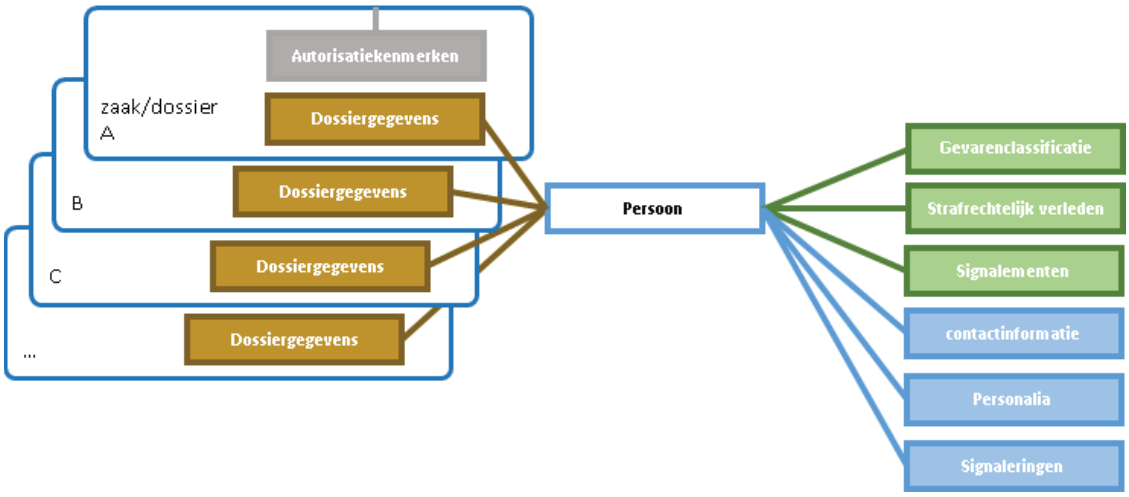
Afhankelijk van de kwaliteit van gegevensdiensten van de overheidsregistratie kan een andere invulling gegeven worden. In veel gevallen zal het nodig zijn om binnen de politie 'compenserende maatregelen' te treffen in het koppelvlak omdat betreffende overheidsregistratie niet aan de gestelde kwaliteitseisen kan voldoen. Dit kan bv door een 'kloon' van de overheidsregistratie te verkrijgen.

Aannemelijk is dat dit in alle gevallen noodzakelijk is. Aanvullende reden is dat we ook voor de externe gegevensobjecten het semantisch model politie (SMP) volgen. En op dit moment is het SMP ongelijk aan de semantisch modellen van de overheidsregistraties. Dat gaat ook niet gebeuren, omdat we gelijkvormigheid over gegevensobjecten van hetzelfde soort "ding" willen hebben, terwijl de modellen van de BRP, SKDB en BVV bv zullen blijven verschillen.

Het BOR zal ontsloten moeten worden naar de intel om de informatiepositie compleet te houden.

Gedistribueerde kennis over '1 ding in de werkelijkheid' zal geaggregeerd moeten worden bij de intel om een compleet beeld (informatiepositie) te krijgen. Dat betekent dat:

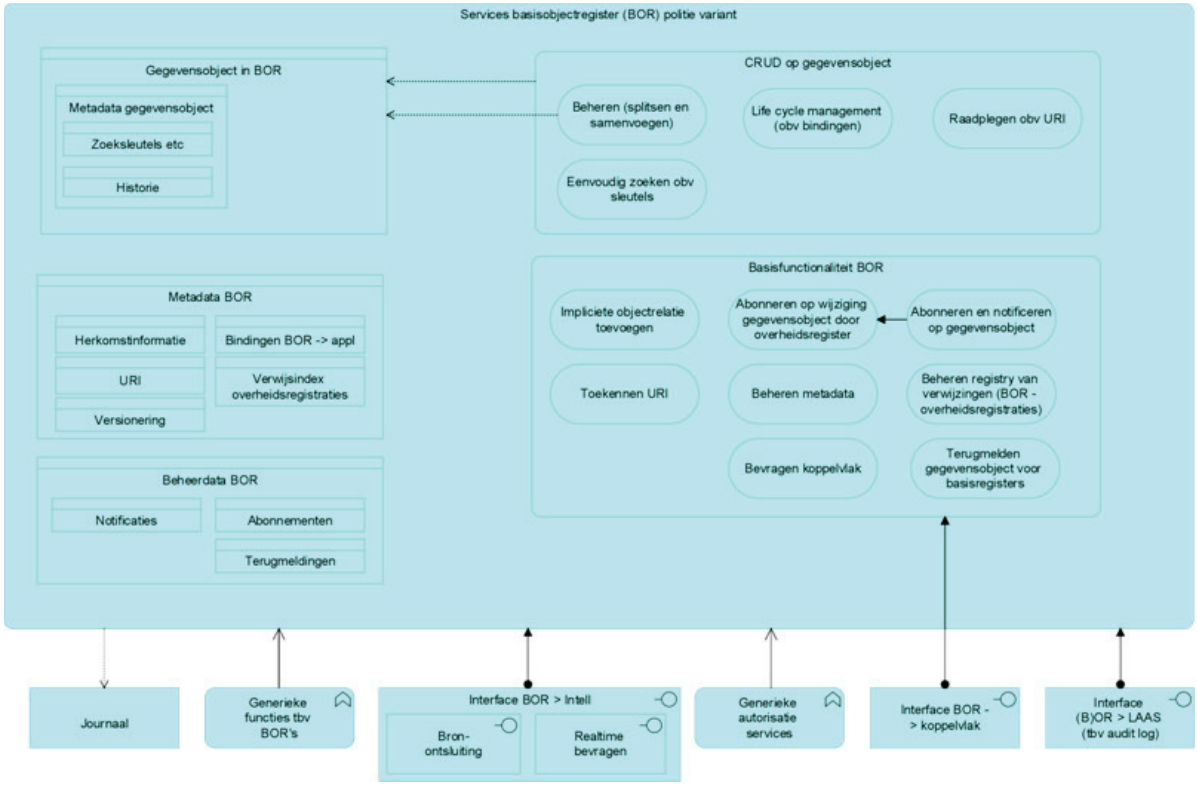
- De verwijsindexen van een BOR worden als bron ontsloten zodat de intel de aggregatie kan verzorgen.
- De intel past de autorisatieregels toe op basis van de autorisatiecontext van de zaak.



Zie ook Afhankelijkheden met intel

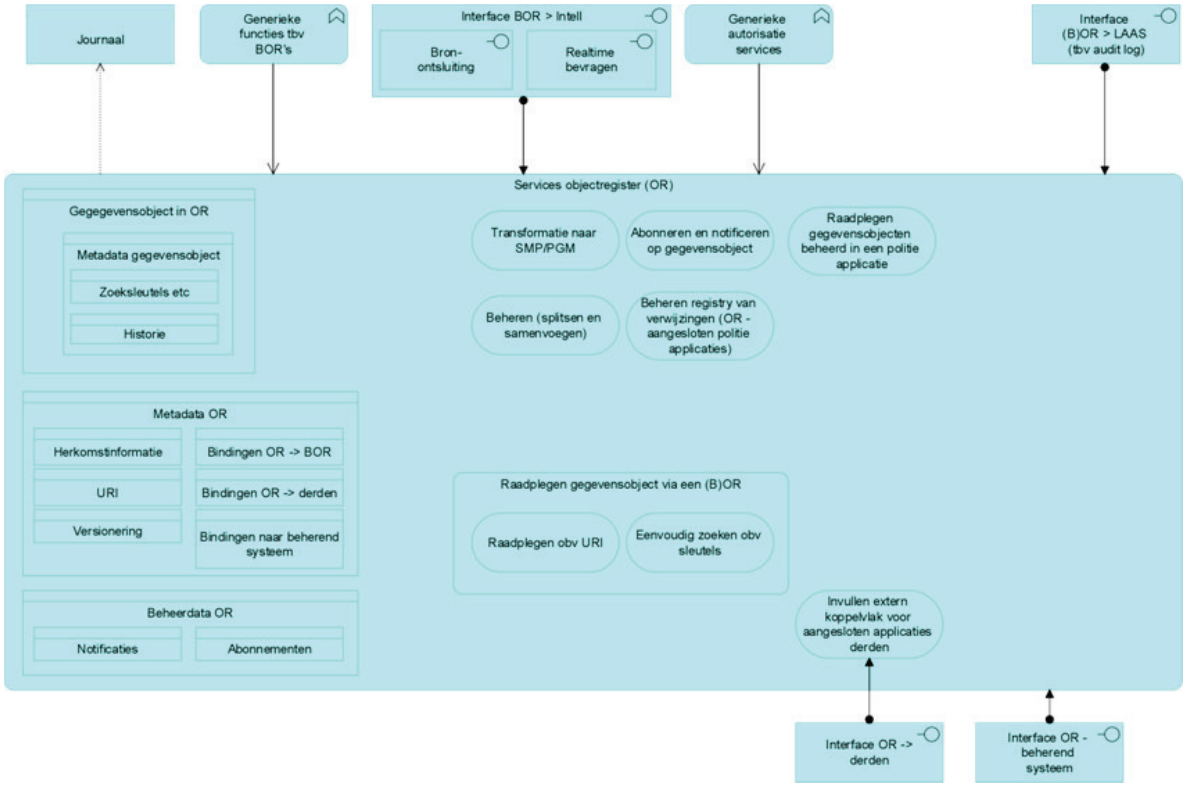
Functionaliteit van een basisobjectregister

Onderstaand schema beschrijft de gegevens, functionaliteit en interfaces, te implementeren per BOR.

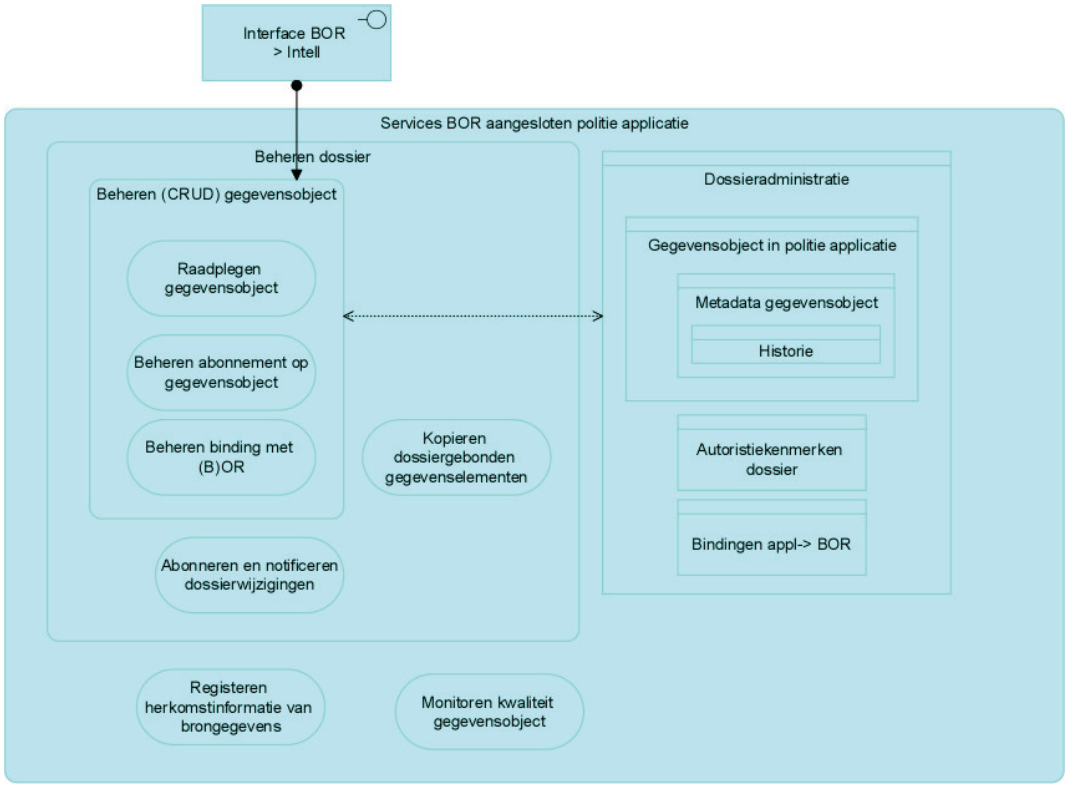


Functionaliteit van een objectregister

Onderstaand schema beschrijft de gegevens, functionaliteit en interfaces, te implementeren per OR.



Functionaliteit van een applicatie die op een BOR is aangesloten



Datum besluit	Onder mandaat van	JIRA verwijzing	Contactpersoon	Opmerking (bv wijziging tov vorig besluit)
		INFTA-1523 - Getting issue details... STATUS	5.1.2.e	

Datum besluit	Onder mandaat van	JIRA verwijzing	Contactpersoon	Opmerking (bv wijziging tov vorig besluit)
//24-06-2021	5.1.	ARCHSE-986 - Getting issue details... STATUS	5.1.2.e	Begrip verplaatst en aangescherpt voor de MDM context.

GBA autorisaties binnen de politie

0577

«waakzaam en dienstbaar»

POLITIE

Wat zijn autorisaties

- **afspraken tussen RvIG en Politie als het gaat om gebruik van gegevens in het GBA, incl. technische borging dat hiervan niet wordt afgeweken.**

- **Er bestaan afspraken voor 3 verschillende doelen**
  - Regulier
    - Afnemersindicatie is zonder meer zichtbaar
  - Gevoelig
    - Afnemersindicatie is zichtbaar voor burger zelf en gemeenteambtenaar
  - Geheim
    - Afnemersindicatie is alleen zichtbaar voor klein aantal gemeenteambtenaren

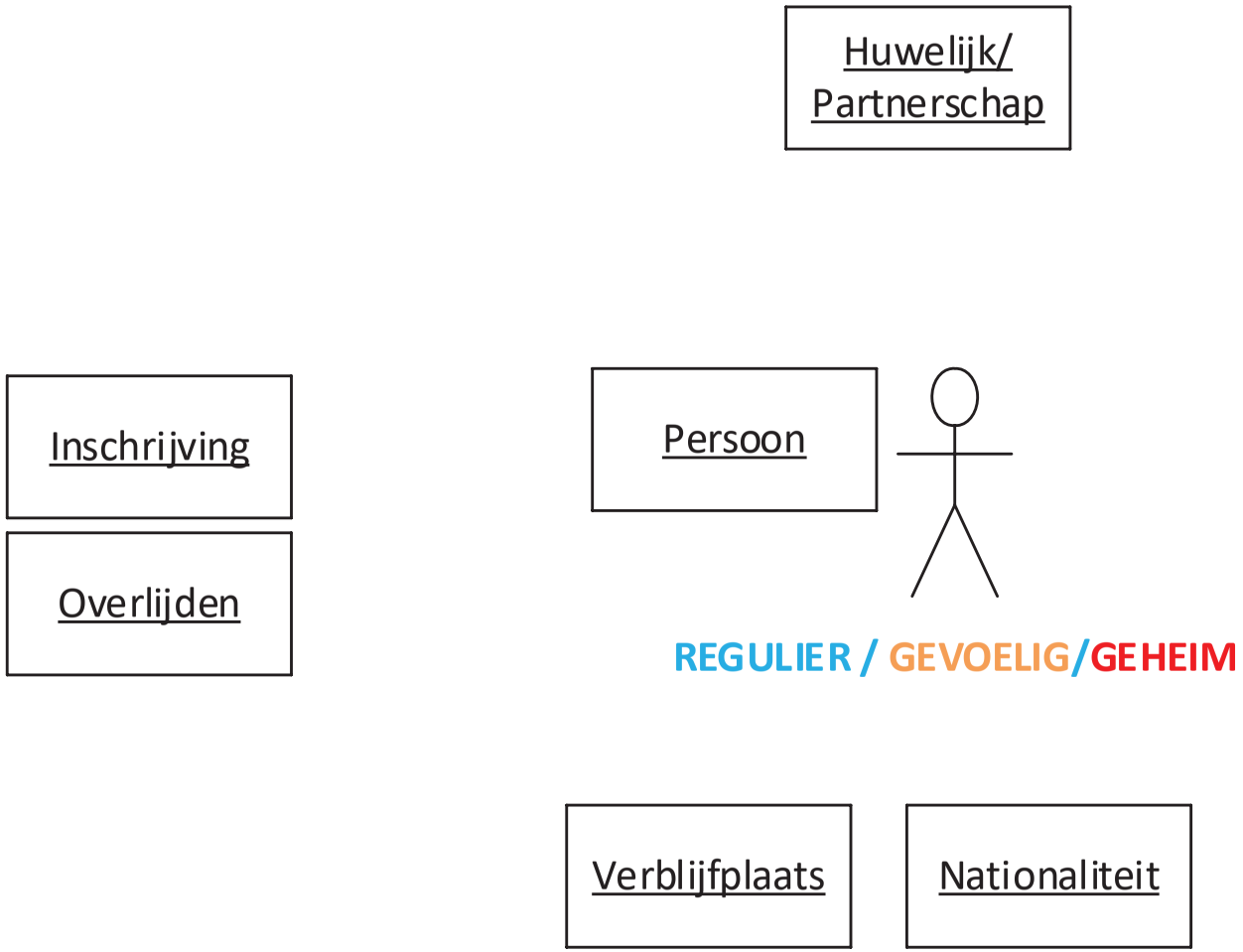
Wat bevatten ze

Definitie welke gegevensrubrieken bij de autorisatie beschikbaar mogen komen op welk moment

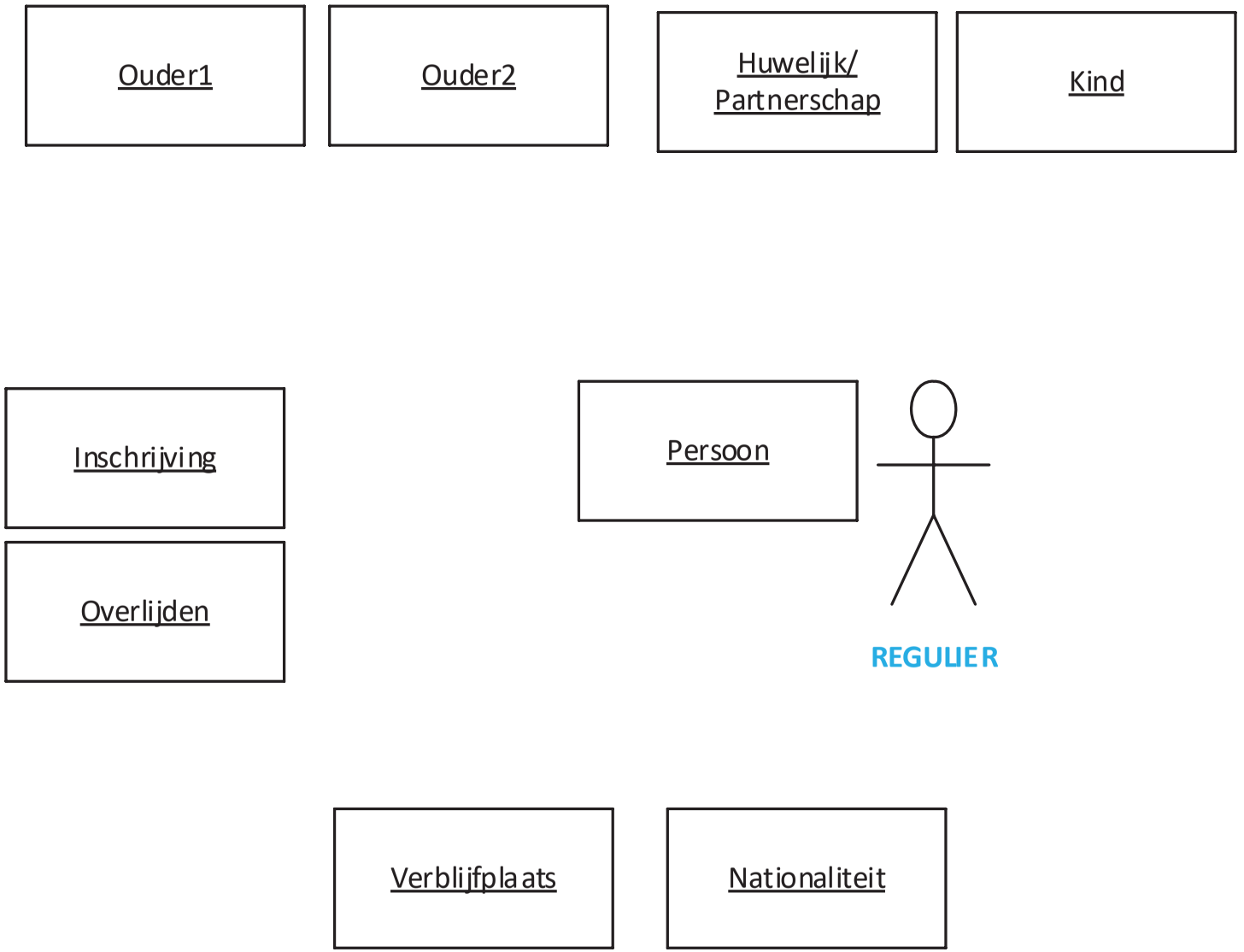
- Spontane verstrekking, bijlage 1 gegevens
- Gegevens op verzoek, bijlage 2 gegevens
- Adresgegevens op verzoek, bijlage 1 gegevens

Rubrieken zijn onderverdeeld in categorien

Regulier/Gevoelig/Geheim (bijlage 1)



Regulier (Bijlage 2)



Geheim/Gevoelig (Bijlage 2)

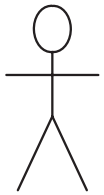
Ouder1(hist)	Ouder2 (hist)	Huwelijk / Partnerschap (hist)	Kind(hist)	Gezagsverhouding (hist)
Ouder1	Ouder2	Huwelijk / Partnerschap	Kind	Gezagsverhouding

Inschrijving

Overlijden

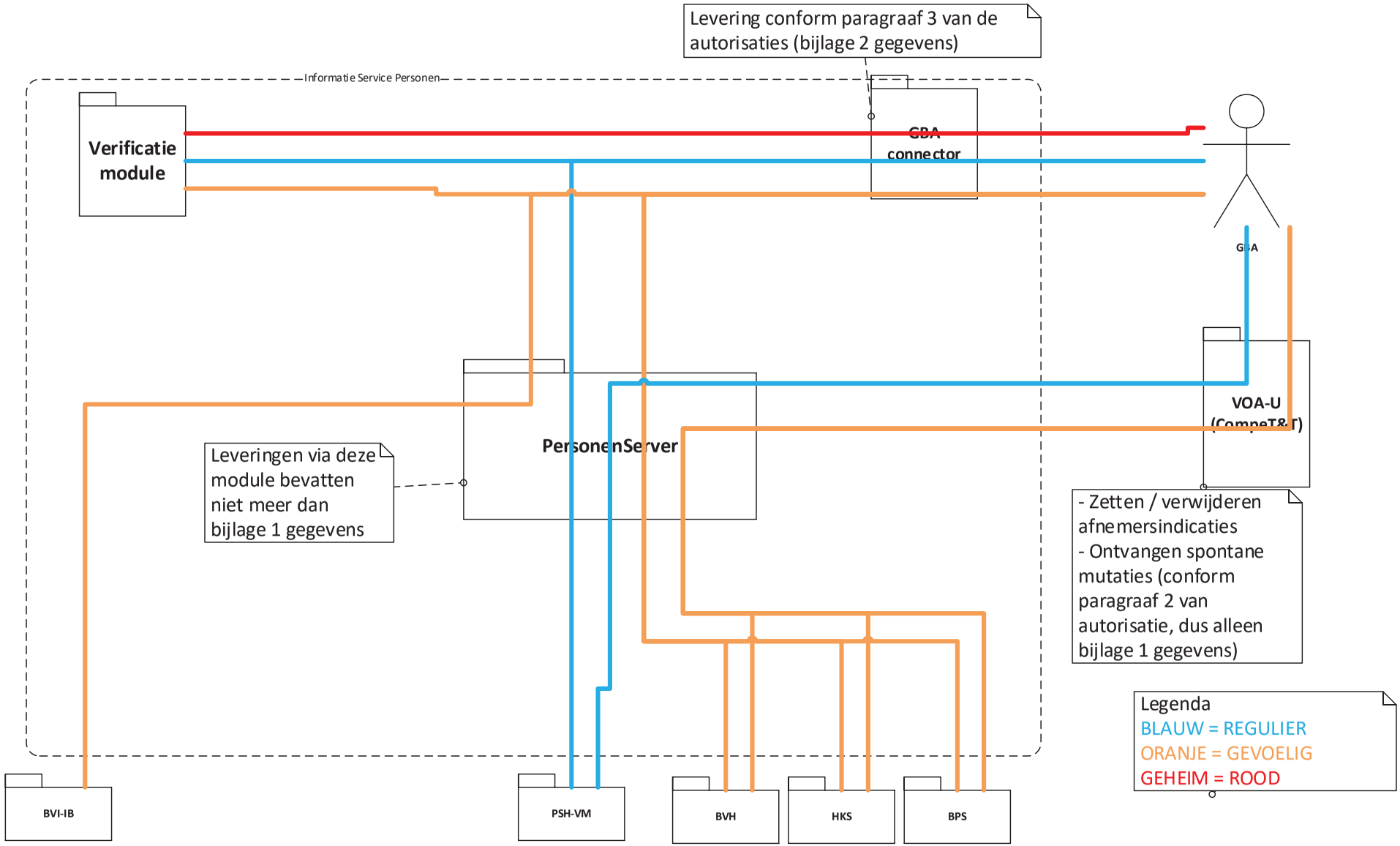
Persoon

Persoon(hist)



GEHEIM / GEVOELIG

Verblijfplaats	Nationaliteit	Reisdocument	Verblijfstitel
Verblijfplaats (hist)	Nationaliteit (hist)		Verblijfstitel (hist)


Levering conform paragraaf 3 van de autorisaties (bijlage 2 gegevens)
Informatie Service Personen
Verificatie module
GBA connector
GBA
VOA-U (CompeT&T)
PersonenServer
Leveringen via deze module bevatten niet meer dan bijlage 1 gegevens
- Zetten / verwijderen afnemersindicaties
- Ontvangen spontane mutaties (conform paragraaf 2 van autorisatie, dus alleen bijlage 1 gegevens)
Legenda
BLAUW = REGULIER
ORANJE = GEVOELIG
GEHEIM = ROOD
BVI-IB
PSH-VM
BVH
HKS
BPS

Vragen?

GBA

Algemeen

Niet onder reikwijdte

Autorisatieniveaus GBA

Voor de bevragingen aan de GBA worden drie soorten niveaus van autorisatie onderkend:

- Regulier
  Deze autorisatie wordt bijvoorbeeld voor het opvragen van gegevens ten behoeve van vergunningen gebruikt.
- Gevoelig
  Deze autorisatie wordt standaard gebruikt voor alle reguliere politiewerk.
- Geheim
  Deze autorisatie wordt gebruikt als het voor de burger geheim moet blijven dat gegevens uit de GBA worden opgevraagd. Bijvoorbeeld bij rechercheonderzoeken.

Niet onder reikwijdte

Beheer van de Verificatiemodule

De regionale beheerder van de Verificatiemodule zal vragen over de applicatie of de betekenis van de gegevens gaarne beantwoorden. Ook eventuele problemen of wensen voor verbetering van de applicatie en de bijbehorende helptekst worden door de regionale beheerders van elk korps behandeld.

Er is voor het gebruik van deze applicatie geen handleiding beschikbaar. Alle noodzakelijke informatie is verwerkt in de helptekst. Als de helptekst om welke reden dan ook de gebruiker onvoldoende informeert, zal deze aangepast worden. Wensen op dit punt gaarne doorgeven aan de regionale beheerder van het korps.

Niet onder reikwijdte

>>>

Zoeken

Niet onder reikwijdte


Niet onder reikwijdte

Niet onder reikwijdte

Basisobjectregister Persoon

MDM 2e iteratie

Intentionele Architectuur → Emergent design

Versie 1.1

Slide 2 tot en met 11 valt niet onder de reikwijdte van het verzoek

Niet onder reikwijdte

Complicatie t.a.v. BOR Persoon

- In OPP is een module voor personenregistratie gebouwd die niet voldoet aan de architectuur van een BOR
- Met deze module zijn persoonsgegevens opgeslagen die modelmatig niet correct zijn volgens de BOR architectuur waardoor een correctie moet worden toegepast op de gegevens
- De persoonsgegevens worden uit de personenserver (koppelvlak) gehaald als koppelvlak, maar bedienen niet de legacy of geven geregistreerde gegevens uit OPP terug aan de personenserver
- Het koppelvlak met basisregistratie BRP is onder scherpe media aandacht i.h.k.v. bovenmatig gebruik van gegevens door de politie
- Het koppelvlak bedient legacy applicaties waardoor de BOR terugmeldingen met additionele logica naar het koppelvlak moet realiseren
- Het BOR deelt een uniek nummer uit voor personen ter hergebruik, het bestaande P-Nummer vanuit het koppelvlak heeft eenzelfde status. Het P-Nummer zou in de toekomst door het BOR kunnen worden uitgegeven, dit is op dit moment nog niet bepaald.
- De CIO en Regie Board generieke voorzieningen hebben voor 2022 een beperkt urenbudget beschikbaar gesteld om de personenserver aan te passen naar gestelde kaders tegen bovenmatig gebruik van gegevens
- Als afnemer van gegevens heeft de politie een terugmeldplicht. Het proces van terugmelden is door de bijzondere positie van de politie mensenwerk. Het BOR zal door goede administratie van gegevens dit proces ondersteunen, maar niet automatiseren.
- De personenserver werkt persoonsgegevens automatisch bij (ook wel een afnemersindicatie genoemd) deze functionaliteit is niet wenselijk voor een BOR omdat een BOR gegevens pas bij gebruik (op basis van nut en noodzaak) ophaalt uit basisregisters.

Slide 13 tot en met 49 valt niet onder de reikwijdte van het verzoek

Two Pager Informatie uitwisseling Belastingdienst – politie

Aanleiding
Follow the Money publiceerde op 10 oktober het artikel 'De politie vraagt opvallend vaak gegevens op van toeslagenouders, maar kan niet zeggen waarom'.[1] Naar aanleiding van die publicatie zijn verschillende Kamervragen gesteld en is de politie gevraagd om dit bericht nader te duiden. De politie heeft – mede i.v.m. het Commissiedebat politie d.d. 20 oktober – al een eerste reactie gegeven, met de toezegging een en ander nader uit te zoeken. Dit document bevat een nadere toelichting waarbij ook input van de eenheden is verwerkt.

Kern
De gedupeerden van de toeslagenaffaire vormen geen aandachtsgroep voor de werkzaamheden van de politie en dat is in het verleden ook niet het geval geweest. Bij het initiële contact tussen een politiefunctionaris en een persoon (of deze persoon nu in hoedanigheid van verdachte, slachtoffer, benadeelde, getuige, onderhevig is aan politiecontrole of omstander is) is voor de politiefunctionaris niet kenbaar of de betrokkene in kwestie wel of geen gedupeerde van de toeslagenaffaire is. Bij het verwerken van gegevens naar aanleiding van een dergelijk contact wordt dit dan ook niet geregistreerd.

De politie kan niet nagaan of erkende gedupeerden van de toeslagenaffaire bovenmatig veel in bevragingen in de Basisregistratie Personen (BRP) vanuit de politie voorkomen, omdat gedupeerden niet als zodanig staan geregistreerd bij de politie. Oftewel; de politie weet niet wie betreffende gedupeerden zijn. Als een individuele gedupeerde wil weten welke gegevens van hem of haar bij de politie bekend zijn, dan kan de gedupeerde daartoe een inzageverzoek bij de politie doen. Over afnemersindicaties is de Kamer recent geïnformeerd middels beantwoording van de Kamervragen van het lid Simons (BIJ1) over het ingezette beleid vanuit de politie om het aantal automatische BRP-bevragingen zoveel als mogelijk tot het minimum te beperken. Ik verwijs u naar de antwoorden op deze Kamervragen.

Gegevensuitwisseling Belastingdienst - Politie
Gegevensverstrekking vindt plaats op twee gronden. De politie kan *in het kader van strafrechtelijk onderzoek* gegevens opvragen bij de Belastingdienst en Toeslagen. Alleen de Belastingdienst en Toeslagen weten in dit geval van de gegevens die zij aanleveren uit welke systemen deze afkomstig zijn.

Daarnaast bestaan er *diverse convenanten en samenwerkingsverbanden* op basis waarvan gegevens worden uitgewisseld door overheden, ook tussen de Belastingdienst/Toeslagen en de politie. Op eenheidsniveau wordt samengewerkt binnen het verband van een *Regionaal Intelligence en Expertisecentrum (RIEC)*. Op zaaksniveau vindt gegevensuitwisseling plaats tussen de deelnemers van een RIEC, zoals tussen de Belastingdienst en de politie. Deze gegevensuitwisseling vindt alleen plaats voor de doelstellingen van het RIEC en onder de werking van het RIEC convenant en privacy protocol (bijgevoegd). Daarnaast werken de politie en de Belastingdienst samen op basis van de *Landelijke 'Samenwerkingsovereenkomst voor Interventieteams 2017' (LSI)*.

Het voornaamste convenant waarop informatie-uitwisseling plaatsvindt *betreft het landelijk convenant (bijgevoegd) voor het aanleveren van gegevens door de Belastingdienst aan de Politie ten behoeve van het samenstellen van referentielijsten voor ANPR*. De Belastingdienst maakt bij die samenwerking gebruik van de ANPR apparatuur van de politie. Daartoe voorziet de Belastingdienst de politie van

[1] https://www.ftm.nl/artikelen/politie-monitort-gedupeerden-toeslagenaffaire?share=7%2Bkiq5YCoqNxWNyjb2oDThUixFo8%2FXFtQvPYP5pogWw7we%2BIk93MA%2BH3ZBSAIMk%3D

een bestand met kentekens van schuldenaren van de Belastingdienst. De politie laadt die gegevens tijdelijk en uitsluitend voor betreffende gezamenlijke actie in de ANPR apparatuur van de politie in. De Belastingdienst is zelf verantwoordelijk voor de aangeleverde gegevens en de politie weet niet op basis van welke bron de belastingschuld van de kentekenhouder aan de Belastingdienst is ontstaan. Het gaat hier altijd om een gezamenlijke verkeersactie tussen de Belastingdienst en de politie, waarbij op basis van een ANPR hit een verkeersdeelnemer door ofwel de politie ofwel de Belastingdienst wordt gecontroleerd. In bijgevoegde brief uit 2018 zijn de richtlijnen opgenomen waaraan het gebruik van ANPR door de Belastingdienst en politie dient te voldoen, namelijk;

- er is sprake van een strikte scheiding tussen wettelijke taken en bevoegdheden die een ieder uitvoert tijdens en gezamenlijke actie;
- alvorens deze gezamenlijke actie plaatsvindt, levert de Belastingdienst kentekenbestanden aan zonder vermelding van naam en adres van de belastingschuldige (die tijdens de controle (veelal) op een politie laptop staan);
- de politie kan deze referentielijsten door middel van ANPR-software gebruiken bij zowel de eigen opsporingstaak als de ondersteuning bij de invordering van rijksbelastingen en toeslagen;
- in geval van een hit op één van de bestanden, zal de afwikkeling ter plaatse door ambtenaren van de Belastingdienst geschieden. In de normale gang van zaken geeft de politie enkel het stopteken aan het betreffende voertuig;
- de politie zorgt ervoor dat de referentiebestanden (en daarmee de daaraan ten grondslag liggende gegevens), worden vernietigd zodra zij niet meer in het kader van de wettelijke taken die aan de Politie zijn opgedragen, beschikbaar mogen zijn. Er vindt aldus geen opslag van gegevens plaats in politiesystemen.

In de praktijk betekent bovenstaande dat er sprake is van een gecoördineerd werkproces waarbij vooraf wordt besloten met welke set (ANPR-apparatuur), met welke referentielijst vanuit de belastingdienst, op welke dag en tijdsbestek én op welke locatie een gezamenlijke actie plaats gaat vinden. De vertegenwoordiger(s) vanuit de Belastingdienst zijn gedurende de gehele gezamenlijke actie fysiek aanwezig.

Tot slot

De politie heeft bij de uitvoering van de politietaak (artikel 3 Politiewet) geen bijzondere aandacht voor de gedupeerden van de Toeslagenaffaire. Het is voor de politie bij de gegevensuitwisseling met de Belastingdienst ook niet zichtbaar of het gaat om gedupeerden van de Toeslagenaffaire. De politie heeft immers niet een overzicht met de namen van de personen die tot deze doelgroep behoren. Ook uit overige gegevens die de politie van de Belastingdienst ontvangt is voor te politie niet te herleiden of het hier gaat om deze doelgroep.

Relevante documenten


convenant_belasti


Brief Belastingdie


PrivacyprotocolA\


Convenant inclus

Basis Object Register

Eenmalig opslag en beheer, meervoudig gebruik.

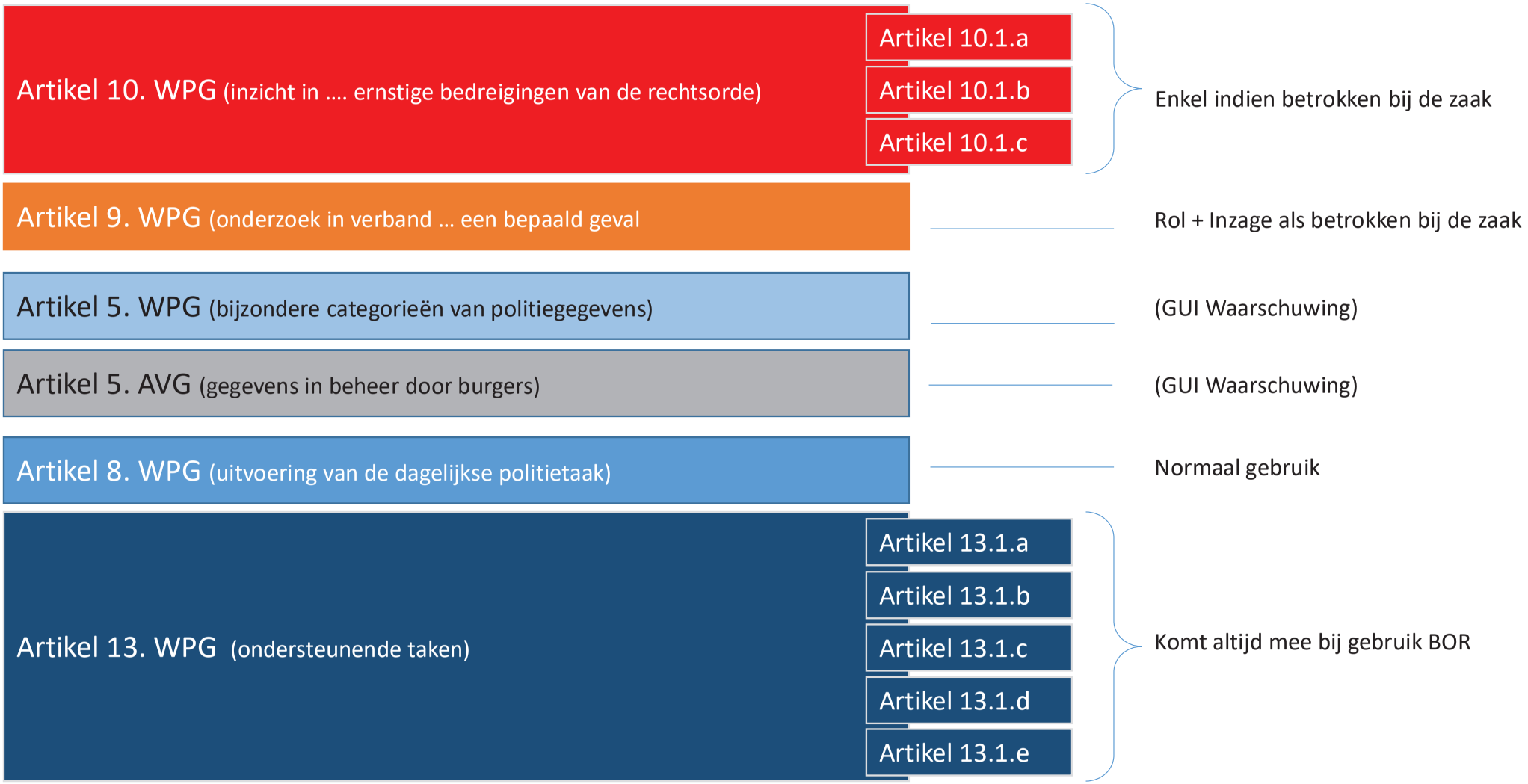
Wat is een BOR en wat kan je ermee?

- Een BOR is een **technische** voorziening in het leven geroepen om gegevens die we als politie vastleggen **efficiënt** te beheren en benaderbaar te maken
  - Eenmalig vastleggen
  - Meerdere keren gebruiken
  - Gegevens niet langer bewaren dan wat mag
- Het is een digitale versie van een **ouderwetse archiefkast**
  - Meerdere lades, met en zonder sleuteltje
  - Meerdere mapjes in een lade
  - Toegang op basis van autorisatie
- De inhoud van iedere archiefkast gaat over **1 ding in de werkelijkheid** (persoon, voertuig, locatie, bedrijf etc)

PVR definitie van een BOR

Een BasisObjectRegister is een fysiek **register** waarmee alle voor de politie relevante **kenmerken** van één specifiek **gegevensobject** centraal worden beheerd en kan worden ontsloten voor **(her)gebruik**.

Samenvatting van alle lades in een BOR



Lades op basis van de Algemene Verordening Gegevensbescherming & Wet Politie Gegevens + werkzaam bij politie en executief

Samenvatting van alle lades in een BOR (andere volgorde.)

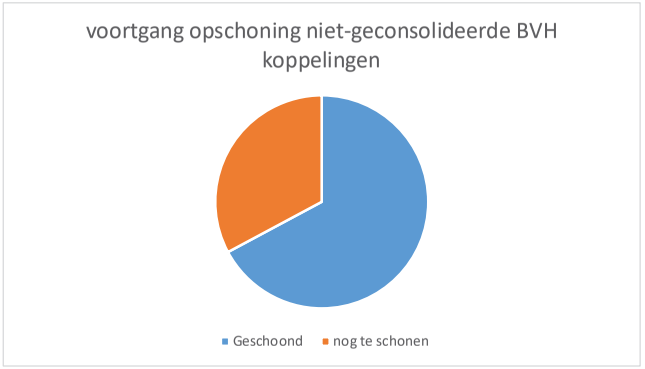
Lades op basis van de Algemene Verordening Gegevensbescherming & Wet Politie Gegevens + werkzaam bij politie en executief

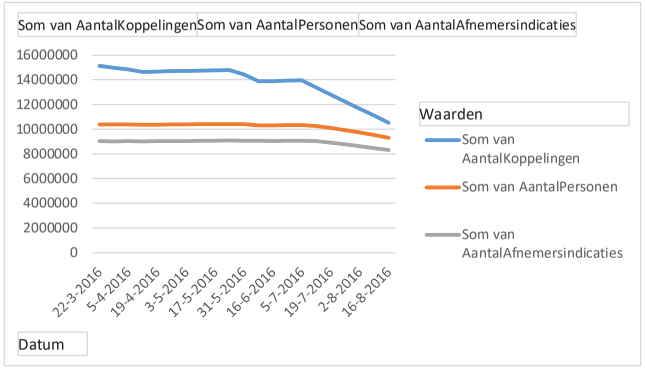
Samenvatting mogelijke gegevensstromen

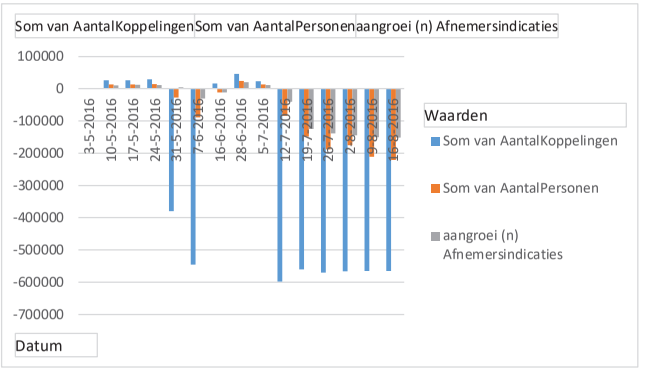
Alle lijnen en pijlen zijn onderhevig aan protocollen

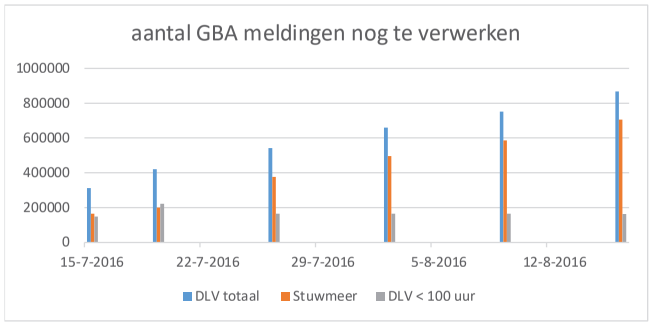
Regio BVH	Eenheid BVH	aantal personen met pnr uit gba	totaal aantal personen	%	aant. pers. die wel persserv koppeling hebben,maar niet in eenheid BVH staan
aml	**aml**	**697065**	**1168557**	**59,7**	
bbn	**bbn**	**531415**	**598484**	**88,8**	
bzo	bbn	427616	482297	88,7	314927
drn	grn	232562	250129	93	159816
frl	grn	407556	767709	53,1	306192
fvl	utr	318827	509694	62,6	232968
glm	nog	336299	397571	84,6	237372
glz	nog	269655	316553	85,2	201207
gnv	utr	143946	158355	90,9	97448
grn	**grn**	**556823**	**624360**	**89,2**	
hgl	**hgl**	**814292**	**954565**	**85,3**	
hlm	hgl	390808	438452	89,1	278452
ijs	nog	286407	296272	96,7	200943
ken	zaw	300284	335690	89,5	221869
klp	**klp**	**300284**	**335690**	**89,5**	
lbn	**lbn**	**431151**	**542653**	**79,5**	
lbz	lbn	377319	929779	40,6	276194
mwb	**mwb**	**724827**	**906094**	**80**	
nhn	zaw	293800	330881	88,8	211567
nog	**nog**	**907633**	**957570**	**94,8**	
rnm	**rnm**	**962568**	**2046869**	**47**	
twn	nog	309177	337461	91,6	215986
utr	**utr**	**881447**	**983199**	**89,7**	
zaw	**zaw**	**452543**	**511851**	**88,4**	
zhz	rnm	198939	238624	83,4	119609
zld	mwb	189520	232451	81,5	133528
		Totaal aantal unieke persoon abo's die we kwijt raken:			3041149

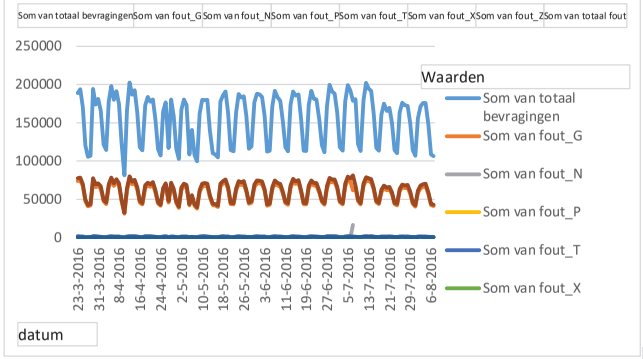
= 3 miljoen!


voortgang opschoning niet-geconsolideerde BVH koppelingen
Geschoond
nog te schonen

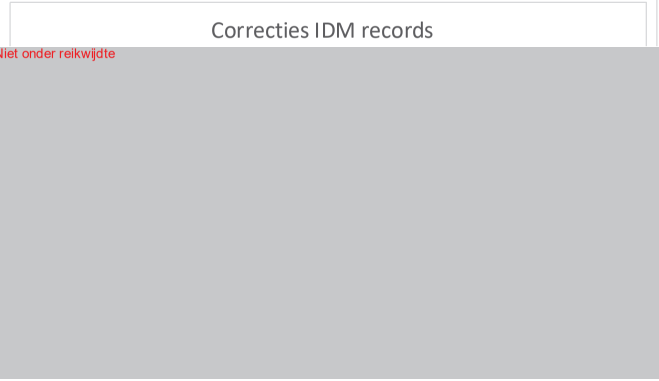

Som van AantalKoppelingen
Som van AantalPersonen
Som van AantalAfnemersindicaties
16000000
14000000
12000000
10000000
8000000
6000000
4000000
2000000
0
22-3-2016
5-4-2016
19-4-2016
3-5-2016
17-5-2016
31-5-2016
16-6-2016
5-7-2016
19-7-2016
2-8-2016
16-8-2016
Waarden
Som van AantalKoppelingen
Som van AantalPersonen
Som van AantalAfnemersindicaties
Datum


Som van AantalKoppelingen
Som van AantalPersonen
aangroei (n) Afnemersindicaties
100000
0
-100000
-200000
-300000
-400000
-500000
-600000
-700000
3-5-2016
10-5-2016
17-5-2016
24-5-2016
31-5-2016
7-6-2016
16-6-2016
28-6-2016
5-7-2016
12-7-2016
19-7-2016
26-7-2016
2-8-2016
9-8-2016
16-8-2016
Waarden
Som van AantalKoppelingen
Som van AantalPersonen
aangroei (n) Afnemersindicaties
Datum


aantal GBA meldingen nog te verwerken
1000000
800000
600000
400000
200000
0
15-7-2016
22-7-2016
29-7-2016
5-8-2016
12-8-2016
DLV totaal
Stuwmeer
DLV < 100 uur


Som van totaal bevragingen
Som van fout_G
Som van fout_N
Som van fout_P
Som van fout_T
Som van fout_X
Som van fout_Z
Som van totaal fout
250000
200000
150000
100000
50000
0
23-3-2016
31-3-2016
8-4-2016
16-4-2016
24-4-2016
2-5-2016
10-5-2016
18-5-2016
26-5-2016
3-6-2016
11-6-2016
19-6-2016
27-6-2016
5-7-2016
13-7-2016
21-7-2016
29-7-2016
6-8-2016
Waarden
Som van totaal bevragingen
Som van fout_G
Som van fout_N
Som van fout_P
Som van fout_T
Som van fout_X
datum


Som van aantal
aantal autorisaties
Niet onder reikwijdte


Correcties IDM records
Niet onder reikwijdte


Som van aantal
autorisaties over de eenheden
Niet onder reikwijdte

Overzicht aantal koppelingen, personen, afnemerindicaties

Datum	Koppelingen	Personen	Indicaties	
20160322	15129018	10392820	9031189	
20160329	14962250	10373361	9019017	
20160405	14840631	10375582	9026799	
20160412	14639226	10348422	9014078	
20160419	14667337	10362616	9026132	
20160428	14702494	10380008	9041080	
20160503	14714995	10388044	9048056	
20160510	14741124	10400548	9058203	
20160517	14767050	10413452	9070126	
20160524	14795527	10427634	9080986	
20160531	14416017	10399572	9085459	
20160602	14256105	10373600	9076729	
20160607	13870653	10310442	9054304	
20160616	13886900	10298355	9042153	
20160628	13933000	10321897	9061649	
20160705	13955973	10335284	9073063	
20160712	13358406	10251144	9032252	Schoning BVH gestart op 20160705
20160719	12798189	10102715	8906990	
20160726	12228301	9913960	8768152	
20160802	11662416	9738354	8623891	
20160809	11096872	9526822	8473589	
20160816	10531911	9305587	8322375	
20160823	9985287	9085374	8173456	
20160830	9984570	8938167	8025351	
20160906	10006565	8796257	7881184	
20160913	9672662	8633748	7735378	
20160920	9227256	8450873	7588384	Schoning BVH afgerond
20160927	9252744	8305320	7440461	
20161004	9274424	8157168	7285535	
20161011	9299471	8015922	7145511	
20161018	9323912	7874158	7001399	
20161025	9348913	7840178	6965090	
20161101	9373396	7858203	6980897	
20161108	9393953	7874871	6995867	
20161115	9419267	7893537	7012224	
20161122	9443630	7911393	7028234	
20161129	9468727	7929492	7043957	
20161206	9489164	7947335	7060328	
20161213	9513408	7964741	7075645	
20161220	9537553	7982488	7091713	
20161227	9558706	7997955	7106587	
20170103	9578606	8015154	7120892	
20170110	9601171	8030941	7135128	
20170117	9624132	8047321	7149754	
20170124	9645926	8063140	7163953	
20170131	9669577	8080380	7178681	
20170207	9690454	8097113	7192816	
20170214	9712907	8113268	7207255	
20170221	9733400	8128179	7221457	
20170228	9756353	8144857	7236390	
20170307	9774749	8159690	7249682	
20170314	9797504	8176160	7264083	
20170321	9820789	8193146	7279302	
20170328	9843876	8210053	7294358	
20170404	9864186	8227643	7309617	
20170411	9888236	8244359	7324292	
20170418	9910590	8260643	7338869	

20170425	9933203	8277217	7353027
20170502	9954244	8292343	7366589
20170509	9972504	8307067	7379419
20170516	9998301	8322964	7393843
20170523	10022267	8339991	7408433
20170530	10043288	8355265	7422167
20170606	10061745	8371489	7436837
20170613	10084675	8387236	7449947
20170622	10119841	8412934	7472383
20170627	10136640	8425306	7483485
20170704	10162767	8444912	7499229
20170711	10191021	8467024	7517505
20170718	10229967	8495381	7534522
20170725	10269537	8523826	7553277
20170731	10304461	8549675	7566873
20170808	10322524	8564639	7581261
20170815	10344295	8580139	7593860
20170822	10364778	8594792	7606790
20170829	10386961	8610572	7619957
20170905	10405049	8626154	7633563
20170912	10426172	8640373	7645752
20170919	10446308	8654741	7657958
20170926	10467483	8669975	7671065
20171003	10487465	8685108	7684248
20171010	10506339	8699495	7696461
20171017	10527633	8715113	7710075
20171024	10549771	8730454	7723359
20171031	10572929	8746860	7738018
20171107	10604200	8772570	7760037
20171114	10627265	8788340	7773422
20171120	10648468	8803257	7785530
20171128	10666122	8818920	7800429
20171205	10683764	8831095	7810608
20171212	10704064	8844777	7822522
20171219	10724322	8859419	7834611
20180102	10762356	8887039	7858374
20180109	10778714	8900655	7870070
20180116	10799434	8914758	7882022
20180123	10819869	8928944	7893889
20180130	10840608	8943520	7906082
20180206	10857625	8957974	7917982
20180213	10877527	8971455	7929734
20180220	10897750	8985385	7941707
20180227	10917050	8998621	7952761
20180305	10931095	9010460	7961952
20180313	10952206	9024975	7974621
20180320	10971624	9038776	7986558
20180327	10992333	9053477	7998276
20180403	11009951	9067123	8010084
20180410	10991422	9063976	8021249
20180420	10985640	9062868	8037855
20180425	10998218	9071252	8044495
20180430	11013645	9083792	8055750
20180508	11033803	9099301	8067915
20180515	11052879	9112398	8079795
20180522	11072010	9123601	8097327
20180529	11094676	9139771	8109502
20180605	11110089	9153663	8121529
20180612	11131099	9168088	8133985

20180619	11151834	9183140	8146747
20180626	11173617	9198379	8159538
20180703	11195305	9213885	8172350
20180710	11214314	9229205	8185140
20180717	11237156	9245222	8197977
20180724	11257353	9259534	8204385
20180731	11277270	9273516	9335090
20180807	11292644	9287282	8212508
20180814	11311541	9299588	8241568
20180821	11331040	9313175	8254401
20180828	11350583	9326748	8265577
20180904	11365270	9339732	8276639
20180911	11384570	9352826	8287200
20180918	11403344	9365873	8297895
20180925	11439361	9391698	8319043
20181002	11468707	9412724	8336160
20181009	11485576	9426428	8347388
20181016	11507430	9441672	8359939
20181023	11529443	9457101	8372602
20181030	11549490	9470944	8384468
20181106	11566001	9485184	8396120
20181120	11609254	9514447	8420630
20181127	11632190	9530532	8432982
20181204	11649491	9544776	8445431
20181213	11676817	9563048	8460903
20181218	11690410	9573028	8469418
20181227	11713704	9588951	8483799
20190104	11731987	9605161	8496332
20190108	11742254	9611477	8501391
20190115	11762903	9625461	8513150
20190122	11783584	9639585	8525013
20190129	11802635	9652805	8536007
20190219	11860513	9694634	8570258
20190226	11880906	9708774	8581826
20190307	11904670	9727737	8597759
20190312	11918346	9736524	8605003

Abonnementen (Intern / Extern)

⚠ **! Deze pagina is onder review. Inhoud en locatie zijn aan verandering onderhevig !**

Abonnementen (Intern / Extern)

Secties binnen Enabler Confluence-pagina (opvouwbaar)

1. Achtergrond/Context (Het "Waarom")

Voor politiewerk is soms noodzakelijk om natuurlijke personen op de hoogte te stellen dat een administratieve gebeurtenis heeft plaatsgevonden. Natuurlijke personen kunnen zowel medewerkers van de politie zijn, mensen werkzaam bij dan wel voor ketenpartners dan wel belanghebbenden als burgers. Bij het onderwerp abonnementen hebben we al snel te maken met zowel de WPG als AVG.

De voorwaarden wanneer dat is noemen we een abonnement. De reden waarom dit nodig is ligt besloten in de context waarin een abonnement is afgesloten. Een abonnement is dus nooit een losstaand iets en altijd te herleiden naar een lopende zaak / dossier die aan de WPG voldoet. Om invulling te geven aan nut en noodzaak voor politiewerk zal een abonnement niet in oneindigheid kunnen bestaan.

1.1. Waarom is dit van belang voor de NP?

Veel politie processen zijn afhankelijk van een goede informatie positie. Een onderdeel van deze positie is dat belanghebbenden actief op de hoogte worden gesteld dat een, voor de abonnee houder, relevante administratieve gebeurtenis heeft plaatsgevonden. Let op: in het verleden staat dit het op de hoogte stellen vaak synoniem met het verstrekken van gegevens aan de abonnee houder.

Vanuit een security en privacy by design gedachte is het verstrekken van gegevens eerder een uitzondering dan regel en het inzien van de wijzigingen eerder een bewuste handeling vanuit de abonnee houder.

1.1.1. Business motivatie

Abonnementen zijn een breed begrip. In context van PVR, hanteren we deze term als verzamelnaam voor activiteiten die betrekking hebben op de administratieve kant om de nut en noodzaak vast te leggen en de voorwaarden wanneer iemand op de hoogte moet worden gehouden dat er een gebeurtenis in administratieve zin zich heeft voortgedaan. Deze gebeurtenissen bestrijken het gehele administratieve scala wat mogelijk is rondom een gegevensobject. Het daadwerkelijk op de hoogte stellen (notificeren) van de natuurlijk persoon of politie proces, behoort niet tot deze administratie.

De reikwijdte van abonnementen omvat alle mogelijke gegevensverwerkingen (Artikel 1 Wet politiegegevens lid c) maar praktisch gezien eerder op het gebied van vastleggen en wijzigen van gegeven liggen. Het inzetten van een abonnement dient altijd een specifiek doel en is noodzakelijk om politiewerk correct uit te voeren. Het maken en beheren van abonnementen, vallen onder een gegevens verwerking zoals bepaald in Artikel 1 Wet politiegegevens lid c. Hierdoor is het nodig om de nut en noodzaak van een abonnement vooraf te hebben bepaald en dit administratief correct vast te leggen en te beheren. Hiernaast geld dat de WPG grondslag, gekoppeld aan het autorisatiemodel, leidend is of iemand een abonnement mag afsluiten op een gegevensobject dan wel een notificatie kan en mag ontvangen dat er iets is gewijzigd.

Zie voor meer details ook: Implementatievoorbeelden van het SMP.

Wat voor soort abonnementen

We onderscheiden twee verschillende gezichtspunten om naar abonnementen te kijken, beide gekoppeld aan het correct uit te kunnen voeren van politiewerk op basis van gebeurtenissen die te maken hebben met het gezichtspunt. Voor beide geld dat op basis van identificerende gegevens, een expliciete instructie is vastgelegd in het abonnement, hoe om te gaan met de gebeurtenis.

Als voorbeeld, een abonnement op een persoon (BOR Persoon) zal plaatsvinden op het BOR identificatienummer voor de identificerende kenmerken. Als hergebruik van de BOR gegevens plaatsvindt dan wel nieuwe gegevens in de BOR bekend worden gemaakt, kan dit reden zijn om een notificatie te krijgen voor dienders die met een bepaalde zaak bezig zijn.

Deze afweging is dus altijd persoonlijk en context afhankelijk. Zo kan voor een zaak het niet relevant zijn om een abonnement op een verdachte te plaatsen en voor een andere zaak weer wel. Dit gaat op voor alle rollen als dit relevant is voor politiewerk.

Het is dan ook belangrijk om een motivatie te kunnen opgeven waarom een abonnement noodzakelijk is waarbij beleid stelt dat een abonnement een middel is om een bepaald doel te bereiken en het middel terughoudend moet worden ingezet.

De gezichtspunten zijn:

- Administratieve wijzigingen van gegevens (ongeacht of deze beheerd zijn door het BOR)
- Veranderingen in relaties

Het afsluiten van een abonnement op een gegevensobject per gezichtspunt zal verschillende acties teweeg brengen die allen gericht zijn om administratieve gebeurtenissen te detecteren.

Administratieve wijzigingen van gegevens (ongeacht of deze beheerd zijn door het BOR)

Als gegevens in politiesystemen verwerkt worden kan dit relevant zijn voor diverse politieprocessen. De scope voor deze gegevens is breder dan enkel politiesystemen. Het omvat ook administratieve wijzigingen in overheidsregisters zoals bijvoorbeeld het BRP.

Te denken valt aan:

5.1.2.i

Veranderingen in relaties

Veranderingen in relaties moeten breed bezien worden. Zo is het leggen van een nieuwe relatie, bijvoorbeeld vanuit een zaak met een BOR of vanuit een zaak met een andere zaak of vanuit een BOR een relatie leggen met een andere BOR, een verandering ten opzichte van een eerdere toestand.

Hierbij moet worden opgemerkt dat een BOR geen kennis heeft waarom (hoedanigheid / rol) een relatie wordt aangebracht vanuit een zaak gezien. Dit is dan ook een aandachtspunt voor deze vorm van een abonnement.

Dit soort abonnementen betreffen al snel complexere gevallen, te denken valt aan:

5.1.2.i

Niet onder reikwijdte

Niet onder reikwijdte

Niet onder reikwijdte

3.1. Waarbinnen moet het wat hoe worden ontwerpen?

Binnen OPP de registratie van abonnementen, binnen BVI de effectuering van abonnementen.

Bijzondere aandacht moet er zijn voor gegevens verwerkingen gerelateerd aan het Basis Object Register (BOR). Of dit nu het leggen van een nieuwe relatie met het BOR betreft dan wel het toevoegen, aanpassen of verwijderen van de gegevens die in een BOR beheerd worden.

Waarom zijn abonnementen nodig voor een BOR?

Het karakter van de BOR is het verlenen van administratieve diensten voor politieprocessen, die ook wel werkstromen worden genoemd. Deze dienstverlening is afgestemd op gebeurtenissen die tijdens de uitvoer van een werkstroom kunnen voorkomen of gebeurtenissen die een bepaalde werkstroom beginnen dan wel eindigen. Het BOR is in zeker zin een brug tussen twee stijlen (gebeurtenis en werkstroom) waarbij een gebeurtenis centraal staat.

Er is op voorhand geen kennis aanwezig in het BOR wat er moet gebeuren bij een bepaalde gebeurtenis. Dit wordt bekrachtigd met diverse beleidsmaatregelen zoals het beleid rondom afnemersindicatie (zie 2.5 Bedrijfsregels BOR, nummer 22) en ook in de privacy en security by design (Privacy & Security by Design) richtlijnen. Uit het Uitvoeringskader Privacy en Security by Design v2.0.pdf, beleidsmaatregelen en richtlijnen (H5.1.5) is op te maken dat kennis en beheer over abonnementen op zo min mogelijk plekken word onderhouden waardoor we voor nu uitgaan dat abonnementen op BOR gegevensobjecten beheerd worden bij het BOR zelf.

Neem als voorbeeld de gebeurtenis “diefstal” en de dienst “aangifte van diefstal”. Voor de dienst “aangifte van diefstal” is de gebeurtenis “diefstal” om twee redenen relevant:
• Allereerst is hier de gebeurtenis het onderwerp van de dienst. Dus, de gebeurtenis staat gemodelleerd in het semantische domeinmodel dat bij de dienst hoort

• Daarnaast is de diefstal in zekere zin de trigger van de dienst, of preciezer gezegd, van de dialoog van de dienst en daarmee ook van het interne proces van de aanbieder van de dienst

• Bij uitvoer van registratie van de diefstal blijkt dat de aangever gezocht wordt voor een getuigenverklaring

De kennis of het noodzakelijk is om van een gebeurtenis kennis te nemen in een andere werkstroom dan waar de gegevens worden verwerkt, ligt bij materie deskundigen en zijn altijd direct gerelateerd aan politiewerk.

Soms wordt naast voornoemde stijlen ook een “gebeurtenis-gerichte” stijl onderkend, waarin het waarnemen en doorgeven van gebeurtenissen een sleutelrol speelt. In zo’n zogeheten event-driven architecture (EDA) geven spelers elkaar events door, door middel van berichten, en veelal met behulp van een publish-subscribe-mechanisme.

Een voorbeeld is de gebeurtenis "verhuizing" van iemand die in een onderzoek staat opgenomen.

• Allereerst is hier de gebeurtenis geen onderwerp van dienstverlening van de politie

• De verhuizing zelf is in zekere zin een trigger van een werkstroom die geen directe relatie lijkt te hebben met de gebeurtenis

• Het onderzoek zal dan ook expliciet moeten aangeven dat dit soort gebeurtenissen die betrekking hebben op het geabonneerde gegevensobject, een trigger zijn voor het onderzoek om een bepaalde werkstroom uit te voeren

• Of de kennis van de soort gebeurtenissen in het event driven mechanisme moeten worden opgenomen is een technische keuze

Het is dan ook zo dat een abonnement alleen kan gebeuren op basis van een reeds bestaande of nieuwe zaak waarin de nut en noodzaak van het abonnement in is beschreven. Het gegeven dat er een abonnement is afgesloten voor een object in het (B)O, volgt altijd dezelfde WPG grondslag waarop de zaak is gebaseerd.

De volgende uitgangspunten zijn altijd van toepassing op abonnementen:

- Een abonnement op een gegevensobject dient altijd politie gerelateerde werkzaamheden zoals bepaald in de Wet Politiegegevens.
- Een bevoegd functionaris bepaald beoordeeld voor de gerelateerde werkzaamheden of een abonnement op dat moment noodzakelijk is.
- Een abonnement is de administratieve vastlegging die direct te relateren is aan een zaak waar de nut en noodzaak van het abonnement in is vastgelegd
- Een abonnement geldt altijd voor 1 gegevensobject en / of
- Een abonnement geldt altijd voor wijzigingen in een informatie product (samengesteld beeld)

Niet onder reikwijdte

Niet onder reikwijdte

Niet onder reikwijdte

Niet onder reikwijdte

Plan van aanpak: Reductie GBA abonnementen

Auteur: 5.1.2.e

Status: concept

Versie 0.2

Documentinformatie

Versiegeschiedenis

Versie	Versie datum	Samenvatting van de aanpassing	Gemarkeerde wijzigingen
0.1	160317	Concept op hoofdlijnen	
0.2	160419	Concept met verdieping	

Distributie

Versie	Verzend datum	Naam	Afdeling / Functie
0.1	160317	5.1.2.e – PfT BVH	DIM-Advies
0.1	160317	PfT Den Haag	DIM-Advies
0.1	160317	5.1.2.e	Dir-IV/GA
0.2	160419	5.1.2.e – PfT BVH	DIM-Advies
0.2	160419	PfT Den Haag	DIM-Advies
0.2	160419	5.1.2.e en 5.1.2.e	DIM-GGB
0.2	160419	5.1.2.e	Dir-IV/GA
0.2	160419	5.1.2.e	DICT/Dienstenmanagement

Review commentaar

Versie	Wanneer	Wie	Functie

Inhoud

Inleiding

Voor u ligt een plan van aanpak om het aantal afnemersindicaties bij de GBA terug te brengen.

De directe aanleiding voor dit plan van aanpak is een gesprek tussen de Rijksdienst voor Identiteitsgegevens (RvIG) en het directoraat-generaal Politie (DGPol) van het ministerie van Veiligheid en Justitie. De RvIG heeft aangegeven dat zij zich zorgen maakt over de afnemersindicaties van personen op de Gemeentelijke Basis Administratie (GBA). Zij hebben in 2015 vastgesteld dat het aantal afnemerindicaties in de negen miljoen loopt en blijft stijgen. De RvIG heeft de vraag gesteld of het noodzakelijk is voor de uitvoering van de politietaak om al deze personen in de GBA te blijven volgen. De Directie-IV heeft vervolgens de Dienst-IM gevraagd met plannen te komen om dit vraagstuk aan te pakken.

Achtergrond

De Personenserver is oorspronkelijk in 2000 ontwikkeld als buffer tussen de politieorganisatie en de GBA wegens de toename in raadplegingen op personen als ook de toentertijd beperkte (technische) communicatie capaciteit. In de loop der tijd is de Personenserver uitgegroeid tot een systeem waar persoonskaarten centraal worden opgeslagen. Daarnaast zijn er Informatievoorzieningen – zijnde alle BVH's, PSH-VM, BPS (KMar) en (voormalige) HKS – die zelfstandig gegevens kunnen toevoegen. Daarbij is ook BVID gekoppeld welke identiteitsvaststellingen toevoegt.
Ook is wet- en regelgeving op het gebied van privacy in de loop der jaren veranderd, maar door andere prioriteitstellingen heeft de ontwikkeling van de Personenserver en andere Informatievoorzieningen hier geen gelijke tred mee gehouden.

De informatievoorzieningen BVI-Integrale Bevraging (BVI-IB) en OPP-Executie & Signalering (OPP-E&S) zijn ook gekoppeld, Deze maken geen gebruik van de persoonskaarten maar – gebruik makend van de communicatie voorzieningen binnen de Personenserver – vragen persoonsgegevens rechtstreeks bij de GBA op. Dit laatste levert geen afnemersindicaties op.

Problematiek

Alle personen opgenomen in bijvoorbeeld BVH – verdachten, getuigen, aangevers etc. – krijgen een persoonskaart binnen de Personenserver. Daarbij wordt tegelijkertijd binnen de GBA een afnemersindicatie bij de persoon aangezet. Deze indicatie wordt gebruikt voor terugmeldingen aan de Personenserver wanneer er binnen de GBA een persoonsgegeven ~~wordt gemuteerd~~wijzigt. In verband met het bijhouden van gegevens, wordt na melding aan de Personenserver ook de mutatie doorgestuurd naar ~~i~~informatievoorzieningen die een relatie met de betreffende persoonskaart hebben.
Deze handelswijze heeft tot gevolg dat er vele miljoenen personen worden "gevolgd" doordat ze een indicatie binnen de GBA hebben.

5.2.1

De Wpg geeft in meerdere artikelen regels aan wanneer gegevens verwijderd of vernietigd moeten worden. Bij deze activiteit behoort een signaal vanuit de POA naar de Personenserver dat de persoonsgegevens niet langer actief te hoeven worden gevolgd. De persoonskaart – en daarbij ook de afnemersindicatie bij de GBA – wordt daarna automatisch vernietigd wanneer na ongeveer 4 dagen geen informatievoorziening aan de persoonskaart (meer) is gekoppeld.

Echter, ~~naar aanleiding van enkele Wpg-compliancy onderzoeken in 2015,~~het is gebleken dat – op PSH-VM na – in de aangesloten ~~Informatie~~voorzieningen ~~niet voldoen aan de Wpg vereisten omdat~~ de functionaliteit voor terugmeldingen – bij verwijdering[1] en vernietiging van gegevens – naar de Personenserver ~~daarin~~ niet is opgenomen. Hierdoor heeft verwijdering en/of vernietiging van persoonskaarten zelden of nooit plaatsgevonden waardoor ook de afnemersindicatie in de GBA blijft bestaan.
Dit laatste strookt ~~weer~~ niet met de Wbp omdat er geen onderbouwde doelbinding gegeven kan worden, zoals het RvIG ook al had vastgesteld.

Omdat het aanpassen van deze ~~Informatie~~voorzieningen – naar verwachting – veel tijd zal kosten, geeft dit document voor de korte termijn activiteiten en tijdspaden aan om tot resultaten te komen.

Structurele oplossingen, zoals het vermijden van afnemersindicaties bij bepaalde categorieën[2] personen, zullen – nadat er hiervoor beleid is opgesteld – via het portfolio~~e~~proces moeten lopen.

[1] De release van BVH die eind maart 2016 beschikbaar komt heeft wel verwijderingsfunctionaliteit, doch excl. terugmelding aan de Personenserver.
[2] Denk hierbij aan aangevers, getuigen etc.

Planningen

Voor de korte termijn wordt er gezocht naar wegen om nog in 2016 het aantal registraties binnen de Personenserver en daarmee ook binnen de GBA terug te brengen ~~naar wat noodzakelijk is voor uitvoering van de politietaak~~. De planning daarvoor zal hierna worden besproken.

Daarnaast moet er aandacht zijn voor de langere termijn, doch daarbij hebben we ook te maken met de Wbrp en de aankomende EU-Algemene Verordening Gegevensbescherming (EU-AVG) en de Richtlijn gegevensbescherming voor opsporing en vervolging. Deze laatste hebben ook invloed op de huidige Wbp en de Wpg en derhalve op een veelheid aan ~~Informatie~~voorzieningen binnen de politie. Activiteiten naar aanleiding van bovenstaande lopen via het portfolioproces en zijn hier niet opgenomen.

5.2.1

Met nadruk wordt erop gewezen dat risico's ten aanzien van start- en doorlooptijden zitten in de personele reorganisatie, de uiteindelijke en effectief in werking zijnde personele bezettingen, uitloop van andere projecten, alsmede potentiele vertragingen door bestuurlijke prioriteiten, financiële middelen en wet- en regelgeving.

Situatie BVH

De meeste GBA-koppelingen ~~komen door~~zijn afkomstig van -BVH. Voor de 11 geconsolideerde BVH's is er een ~~versie van BVH~~release in de maak waarbij afgeronde onderzoeken en registraties ouder dan 5 jaar automatisch worden verwijderd. Deze versie heeft vertraging opgelopen en het is niet beken~~t~~d wanneer deze alsnog wordt ontwikkeld cq. geïnstalleerd. Ook is er *geen* functionaliteit opgenomen om de koppeling met de Personenserver te verwijderen. Zonder deze functionaliteit zullen er geen ontkoppelingen kunnen plaatsvinden en derhalve blijft de afnemersindicatie intact.
Het portefeuilleteam voor BVH is aangeraden om deze ontkoppelfunctionaliteit wel op te nemen omdat anders nog steeds niet aan de Wpg/Wbp-vereisten tegemoet wordt gekomen.

Door het RvIG is ook geconstateerd dat de politie personen, die als overleden geregistreerd staan in de GBA ~~staan geregistreerd~~, nog steeds ~~worden gevolgd~~volgt. Het betreft hier een aantal van 200.000 tot 300.000 personen. Het portefeuilleteam voor BVH is gevraagd ook hier aandacht aan te schenken en dit vooral met de operatie af te stemmen opdat de rationale om te volgen een wettelijke gefundeerde doelbinding heeft en daar waar dit niet kan worden onderbouwd, de koppeling met de Personenserver op de voorgeschreven manier te verwijderen.

Planning korte termijn

Zoals hiervoor aangegeven, is idealiter de benodigde functionaliteit reeds opgenomen in de aangesloten ~~Informatie~~voorzieningen. Helaas is geconstateerd dat dit vaak niet het geval is.

Om toch tot resultaat te komen zijn voor de korte termijn de volgende activiteiten gedefinieerd:

1. HKS (Herkenningsdienst systeem) is sinds 2016 niet meer operationeel binnen de politieorganisatie[3]. Alle politie gerelateerde koppelingen tussen HKS en de Personenserver kunnen daardoor verwijderd worden. Deze activiteit wordt al uitgevoerd door de Dienst-ICT en Dienst-IM.

[3] HKS voor de KMar blijft nog wel operationeel.

2. Door de consolidatie van de BVH omgevingen zijn er 15 BVH omgevingen waarin sinds 2015 geen nieuwe onderzoeken aangemaakt worden. Volgens opgave[4] heeft de stuurgroep BVH besloten dat alle koppelingen vanuit deze omgevingen kunnen worden opgeheven, wat naar verwachting ook tot een afname[5] in afnemersindicaties bij de GBA gaat leiden.

Opgemerkt moet worden dat PSH-VM ongeveer 66.000 registraties kent waarvoor een afnemersindicatie binnen de GBA is aangezet. Hoewel deze afnemersindicatie binnen de GBA als politie-gerelateerd is aangemerkt, is deze indicatie nodig ten behoeve van de werkzaamheden voor Justitie. Dit valt onder de Wpg artikel 13, sub 1e verwerkingen. PSH-VM heeft *wel* een terugkoppeling naar de Personenserver, zodat afnemersindicaties hiermee ook worden beheerd.
Het correct registreren en beheren van deze indicaties – inclusief alle andere PSH-VM registraties – gaat naar verluid onder de EU-Algemene Verordening Gegevensbescherming vallen, waarvoor dan ook te zijner tijd aanpassingen binnen PSH-VM nodig lijken te zijn.

Concreet zijn de navolgende data van belang:

Ad1. Medio Q3-2016 zijn alle afnemersindicaties vanuit de voormalige (politie) HKS'en waar mogelijk uitgezet.

Ad2. Begin Q3-2016 zijn alle niet-geconsolideerde BVH's uitgezet die zijn overgebleven na consolidatie. Medio Q3-2016 begint de opschoning van de Personenserver voor de uitgezette BVH's.

Uiterlijk medio Q4-2016 zijn alle bovengenoemde opschoningen afgerond.

Bij het opstellen van de tijdspaden is van het navolgende uitgegaan: het script voor het verwijderen van de koppelingen tussen de Personenserver en de niet-geconsolideerde BVH's kan ongeveer 100.000 (ont)koppelingen per dag verwerken. Bij een aanname dat er 5 miljoen registraties in de 15 niet-geconsolideerde BVH's zijn, betekent dat dit ongeveer 50 dagen duurt voor de ontkoppeling zelf.

Deze activiteiten leiden er, middels een voorzichtige schatting, toe dat er ongeveer 2,5 miljoen personen niet meer actief worden gevolgd. Dit is dan nog exclusief de potentiele vermindering door de opschoning ~~bij~~ in de geconsolideerde BVH's.

Middelen korte termijn

Voor de korte termijn oplossing wordt al onderzocht of dit enerzijds via reeds lopende projecten kan plaatsvinden en anderzijds dat de werkzaamheden via regulier onderhoud en beheer kunnen worden uitgevoerd. Dit laatste zal dan door de Dienst-ICT moeten gebeuren.

Vanuit de Dienst-IM is capaciteit binnen het portefeuilleteam beschikbaar voor strategisch en tactische coördinatie met andere betrokken portefeuilleteams.

Het huidige ontwikkelteam binnen de Dienst-ICT heeft aangegeven ongeveer 220 uur extra nodig te hebben om de benodigde scripts te ontwikkelen en te testen. Eenmaal in gebruik zijn geen extra uren meer nodig.

Accordering

Zowel het MT-DICT als het MT-DIM wordt gevraagd om:

1. van bovenstaand plan kennis te nemen,
2. akkoord te gaan met het de benodigde 220 extra uren ten behoeve van de Dienst-ICT,
3. akkoord te geven op de uitvoering van dit plan.

[4] Opgave door 5.1.2.e. Rol: Senior Business Expert.

[5] Het verwijderen van een afnemerindicatie gebeurd automatisch als er geen enkele IV meer aan een persoonskaart is gekoppeld.

Aan het MT-DIM wordt bovendien gevraagd om:

1. opdracht te geven aan het portefeuilleteam BVH om de additionele bovengenoemde functionaliteiten, ten behoeve van de ontkoppelingen – en derhalve invulling te geven aan de Wpg/Wbp-vereisten –, te ontwikkelen en te installeren.

Scenario PoC Personen

Inleiding

Onderstaand scenario is bedoeld om de volgende doelstellingen te toetsen.

1. Bewijs dat de architectuur en het informatiemodel van kernregisters werkt.
2. Bewijs dat de architectuur van kernregisters past binnen de architectuur van het OPP platform.
3. Bewijs dat kan worden voldaan aan de Wpg (met vooraf vastgestelde bewaartermijnen?).
4. Bewijs dat met de legacy kan worden gekoppeld met geen of minimale impact op de bestaande POA's.

Gebruikte terminologie

Voorziening	Het systeem dat de persoonsgegevens administreert en de communicatie en afhandeling verzorgt tussen afnemend systeem en basisregistratie. Naam van de voorziening nog nader vast te stellen.
Persoonsgegevens	Kernobjectgegevens over natuurlijke personen vastgelegd en onderhouden in een centrale voorziening.
Gebruiker	Gebruiker van een afnemend systeem van persoonsgegevens. Bijv. een gebruiker van BVH of een gebruiker van E&S.
POA	Proces Ondersteunende Applicatie, afnemend systeem van persoonsgegevens van de Personenserver. Bijv. BVH.
BA	Bevragende Applicatie, afnemend systeem van persoonsgegevens van de voorziening. Bijv. E&S. Exacte naam nog nader vast te stellen.
BRP	Extern systeem dat de GBA-gegevens ontsluit. BRP en GBA-V worden als synoniem beschouwd voor dezelfde basisregistratie. De naam BRP wordt gebruikt.

Met opmerkingen [A1]: 5.2.1

Scenario op hoofdlijnen

De interactie is gebaseerd op de huidige werking tussen POA, Personenserver en BRP ten behoeve van de benodigde ondersteuning van de legacy.

1. POA 1 voegt een persoon toe voor verwerking van een Wpg-artikel 10-zaak en wil een geheime afnemersindicatie.
2. Bevragende applicatie 2 voegt dezelfde persoon toe voor verwerking van een Wpg-artikel 8-zaak en wil een reguliere afnemersindicatie.
3. Bevragende applicatie 2 voegt een gevarenclassificatie aan de opgevoerde persoon.
4. Bevragende applicatie 3 vraagt de persoonsgegevens op zonder het verzoek om een afnemersindicatie te plaatsen. Bevragende applicatie 3 ontvangt de reguliere persoonsgegevens en gevarenclassificatie van deze persoon.
5. POA 1 verwijdert de geheime afnemersindicatie.
6. Bevragende applicatie 2 verwijdert de reguliere afnemersindicatie. De persoon heeft op dit moment geen binding meer met "actieve" zaken en moet uit de voorziening worden verwijderd. Na het verstrijken van de bewaartermijn moet de persoon worden vernietigd.

Met opmerkingen [A2]: 5.2.1

Met opmerkingen [A3]: 5.2.1

Buiten scope van de PoC

- Het registreren/loggen van elke bevraging.
- Het bijhouden van mutatiehistorie.

Met opmerkingen [A4]: 5.2.1

Stap 1: zoek voor verwerking Wpg-artikel 10

Korte omschrijving

Persoon A die niet voorkomt in de voorziening toevoegen voor Wpg-artikel 10 met afnemersindicatie geheim.

Stappen

- Een gebruiker van POA 1 zoekt persoon A voor verwerking van een artikel 10-zaak en wil deze persoon volgen (afnemersindicatie geheim).
- De voorziening kent persoon A nog niet en meldt dat aan de gebruiker.
- De gebruiker voegt de persoon toe aan de voorziening (afnemersindicatie geheim).
- De voorziening zoekt en vindt persoon A bij BRP en plaatst afnemersindicatie geheim.

- De voorziening ontvangt de persoonsgegevens voor afnemersindicatie geheim van BRP, verwerkt deze en deelt deze gegevens met POA 1.
  - ? **Wpg-gerelateerde vraag:** Onder welk Wpg-regime vallen de persoonsgegevens die van de BRP worden ontvangen?

Met opmerkingen [A5]: 5.2.1

Stap 2: zoek voor verwerking Wpg-artikel 8 vanuit ander systeem

Korte omschrijving
Persoon A die voor Wpg-artikel 10 voorkomt in de voorziening en afnemersindicatie geheim toevoegen voor Wpg-artikel 8 met afnemersindicatie regulier.

Stappen
- Een gebruiker van bevragende applicatie 2 zoekt persoon A voor verwerking van een artikel 8-zaak en wil deze persoon volgen (afnemersindicatie regulier).
- De voorziening kent persoon A.
  - ? **Wpg-gerelateerde vraag:** Mag de voorziening aan bevragende applicatie 2 antwoorden met de BRP-gegevens van deze persoon die zijn verkregen voor Wpg-artikel 10? De gegevens van de BRP blijven hetzelfde, ongeacht de grondslag waarvoor de gegevens verwerkt worden.
  - ? **Wpg-gerelateerde vraag:** BRP verstrekt voor afnemersindicatie gevoelig en geheim meer gegevens dan voor afnemersindicatie regulier. Aanname: Deze gegevens mogen niet gedeeld worden in geval er gegevens met afnemersindicatie regulier worden gevraagd. Klopt deze aanname?

Met opmerkingen [A6]: 5.2.1

Met opmerkingen [A7]: 5.2.1

De volgende stappen worden alleen uitgevoerd indien de vastgelegde gegevens niet gedeeld mogen worden.
- De voorziening meldt de gebruiker dat de persoon niet bekend is.
- De gebruiker voegt de persoon toe aan de voorziening (afnemersindicatie regulier).
- De voorziening zoekt en vindt persoon A bij BRP en plaatst afnemersindicatie regulier.
- De voorziening ontvangt de persoonsgegevens van BRP en verwerkt deze.
- De voorziening deelt de gegevens voor afnemersindicatie regulier met bevragende applicatie 2.

Met opmerkingen [A8]: 5.2.1

De volgende stappen worden uitgevoerd als de eerder vastgelegde gegevens gedeeld mogen worden.
- De voorziening deelt de eerder geregistreerde gegevens met bevragende applicatie 2. Alleen de gegevens die beschikbaar zijn voor afnemersindicatie regulier worden gedeeld.
- De voorziening plaatst afnemersindicatie regulier.
- De voorziening ontvangt de persoonsgegevens van BRP en verwerkt deze.
- De voorziening deelt de gegevens voor afnemersindicatie regulier met bevragende applicatie 2. Als er geen gewijzigde gegevens zijn ontvangen voor persoon A, kan deze stap worden overgeslagen.

Stap 3: voeg gevarenclassificatie toe

Korte omschrijving
Persoon A krijgt gevarenclassificatie vuurwapengevaarlijk.

Stappen
- Een gebruiker van bevragende applicatie 2 voegt gevarenclassificatie vuurwapengevaarlijk toe aan persoon A.
- De voorziening registreert de gevarenclassificatie.
  - ? **Wpg-gerelateerde vraag:** Valt de gevarenclassificatie van een persoon onder Wpg-artikel 13?
  - ? **Wpg-gerelateerde vraag:** Mag de gevarenclassificatie altijd gedeeld worden? (Mogen Wpg-artikel 13-gegevens altijd gedeeld worden?) Indien nee: welke eisen worden gesteld aan het mogen delen?
  - ? **Architectuurvraag:** Notificeert de voorziening deze gevarenclassificatie aan POA 1? POA 1 heeft een afnemersindicatie (abonnement op mutaties in GBA-V). Wordt dat gelijk gesteld met een abonnement op persoonsgegevens in de voorziening of biedt de voorziening een fijnmazigere abonnementsfunctie? Bijv. een abonnement op 1 of meer van de volgende categorieën.
    - GBA-V-gegevens (geheel of gedeeltelijk)
    - Gevarenclassificatie
    - Adresgegevens (anders dan van de GBA-V)
    - Alle mutaties op persoonsgegevens die binnen Wpg-artikel 13 vallen. (Evt. ook voor overige specifieke Wpg-artikelen.) Etc.

Met opmerkingen [A9]: 5.2.1
1 d.

Met opmerkingen [A10]: 5.2.1

Met opmerkingen [A11]: 5.2.1

Stap 4: zoek voor verificatie vanuit ander systeem (zonder afnemersindicatie)

Korte omschrijving
Persoon A zoeken voor verificatie, zonder verdere verwerking van de persoonsgegevens, zonder afnemersindicatie. ‘Reguliere’ persoonsgegevens en gevarenclassificatie worden geleverd.

Stappen

- Een gebruiker van bevragende applicatie 3 zoekt persoon A voor verwerking van een artikel 8-zaak en wil deze persoon verder niet volgen.
- De voorziening deelt de gegevens voor afnemersindicatie regulier en de vastgelegde gevarenclassificatie met de bevragende applicatie 3.

Met opmerkingen [A12]: 5.2.1 [redacted]

Stap 5: verwijder afnemersindicatie voor POA 1

Korte omschrijving
POA 1 is niet meer geïnteresseerd in Persoon A.

Stappen

- POA 1 meldt aan de voorziening dat deze niet meer geïnteresseerd is in Persoon A en bijbehorende afnemersindicatie geheim.
- De voorziening verwijderd de afnemersindicatie geheim bij GBA-V.

Voor Persoon A is nog een afnemersindicatie regulier vastgelegd. Persoon A mag nog niet uit de voorziening worden verwijderd.

Met opmerkingen [A13]: 5.2.1 [redacted]

Stap 6: verwijder afnemersindicatie voor afnemende applicatie 2

Korte omschrijving
Afnemende applicatie 2 is niet meer geïnteresseerd in Persoon A. Dit was de laatste applicatie die aan Persoon A refereert.

Stappen

- Afnemende applicatie 2 meldt aan de voorziening dat deze niet meer geïnteresseerd is in Persoon A en bijbehorende afnemersindicatie regulier.
- De voorziening verwijderd de afnemersindicatie regulier bij GBA-V.
- Er wordt in de voorziening niet meer gerefereerd aan Persoon A. Persoon A kan verwijderd worden.
  - **Wpg-gerelateerde vraag:** Hoe worden de termijnen voor verwijderen en vernietigen van persoonsgegevens bepaald?
    Afhankelijk van de Wpg-grondslag één termijn per Wpg-grondslag of kunnen er verschillende termijnen gelden ongeacht de Wpg-grondslag? (Bijv. afhankelijk van het type zaak.)
  - **Wpg-gerelateerde vraag:** Welke persoons(gerelateerde)gegevens moeten allemaal worden verwijderd/vernietigd?
    - Alle GBA-V-gegevens en relaties naar politiegegevens
    - Gevarenclassificaties
    - ...
  - **Architectuurvraag:** Is de voorziening zelf verantwoordelijk voor het verwijderen en vernietigen of is dit een taak voor het platform? (Als de voorziening eigenaar is van de persoonsgegevens, lijkt het logisch dat de voorziening zelf verantwoordelijk is.)
  - **Architectuurvraag:** Is de voorziening verantwoordelijk voor het verwijderen van de **gerelateerde politiegegevens** of is dat verantwoording van de applicatie die die gegevens beheerd? (Bijv. social media accounts in het kader van een social media onderzoek. Of PGA-dossier in het kader van een CTER-onderzoek.)
    Aanname: in de praktijk zullen eerst de zaak en gerelateerde politiegegevens worden verwijderd, daarna als laatste pas de persoon uit het kernregister. Zolang de zaak actief of raadpleegbaar is, wordt de persoon (incl. zaak gerelateerde en gedeelde persoonsgegevens) niet verwijderd.
  - **Scope:** als de Personenserver vervangen moet worden, vallen de gegevens van de ID zuil ook binnen scope. Deze gegevens hebben een eigen verwijder- en vernietigingsregime.

Met opmerkingen [A14]: 5.2.1 [redacted]

Met opmerkingen [A15]: 5.2.1 [redacted]

Met opmerkingen [A16]: 5.2.1 [redacted]

Met opmerkingen [A17]: 5.2.1 [redacted]

Met opmerkingen [A18]: 5.2.1 [redacted]

Stavaza personenserver

0604

Logboek

- 30/11/2015 t (FB pers server)/ (IV-epxert ID)/ (pers). Afspraken:
  - Via IM een business expert ID inzetten. Via ( ). Wordt .
  - Alsnog autom. Ontkoppelen bij artikel 14 in BVH? . Nogo.
- 20/11/2015 verzoek van naar (FB BVH) voor impact analyse ontkopp person H's(15).
- 19/11/2015 Gesprek tussen RiVG en DGPOL.
- 11/01/2016 Gesprek tussen RiVG, DGPol en GA. **Eind Q1 PVA gereed.**
- 08/02/2016 Gesprek met , en voor structurele oplossing.
- 07/02 tel contact met . Hij gaat m mmen hoe wens van business b en. => Via DB BVH/BOSZ?
- 25/02 overleg met , (vervanger). heeft voo ept. Gaat dit o tt r Politie form an diging dat het vanuit IM over gaat nemen.
- maakt voorstel voor PVA.
- Autorisatiebesluiten van Rvig toetsen op verplichtingen voor politie.
- Oplegger bij stappenplan maken en daarna MT DIM, MT DICT en MT CIO
- 18/03 heeft met RvIG afgesproken dat PVA in april mondeling wordt spraak wordt nog gepland.

Achtergrond

- De RvIG (Rijksdienst voor Identiteits Gegevens),toezichthouder BRP (GBA), escaleert op dit moment richting de Nationale Politie, omdat we niet kunnen aantonen dat we personen doelgericht volgen.
- Alle personen die in de personenserver zijn opgevoerd worden automatisch bij het BRP aangemeld en gevolgd.
- In de personenserver zijn ca 10,3 mln unieke personen opgevoerd. Doordat een persoon in meerdere afnemende systemen kan zijn opgenomen, komen er nu 16 mln perskoppelingen voor.
- Van deze 16 mln is de BVH verantwoordelijk voor een ruime 12 mln personen.
- 8,9 mln unieke personen worden gevolgd. 1,4 mln zijn onvolledig of vreemdelingen.
- 0,3 mln zijn overleden waarvan 1475 geen afnemersindicatie.
- Oude BVH's bevatten ongeveer 3 mln afnemerindicaties. Oude BVH's worden 01/06/2016 vernietigd. Residu blijft in BVI staan.
- Met nieuwe BVH release worden onderzoeken automatisch na 5 jaar verwijderd. Ontkoppelen personenserver is daar niet in meegenomen. (*** Schatting aantal)
- Script voor ontkoppelen oude BVH/HKS staat klaar.
- Gebruiker krijgt nu in BVH een notificatie. Die kan hij overigens ook negeren waarna de adres gegevens niet bijgewerkt worden in BVH.
- BVH/HKS/Vergunningenmodule/
- 5.1.2.e is coördinerend business expert ID. (Is deels aan het werk). Nu 5.1.2.e
- Personenserver valt in portefeuille van Den Haag. (Paul Musscher)

Privacy

- **Verplichting om gegevens actueel te houden**
  - Dus we mogen iedereen volgen.
- **Doelgericht volgen eindigt als**
  - Verdachte ingezonden naar OM en OM heeft geen verduidelijkings vragen meer.
  - Uiterlijk bij verwijderen onderzoek.
  - Advies 5.1.2.e : Verwijder abo als na verwijderen. Dat is een controleerbaar en vast moment.

Voorstel

- **Opties voor volgen:**
  - Wpg art 8/9/10/12/13?
  - Alleen verdachten ?
  - Bepaalde groepen (vergunninghouders/…)?
  - Delict afhankelijk (Pedofielen/extremisten/…)?
  - Per verdachte handmatig aangeven?
  - Alleen actuele adres gegevens of ook notificatie?
  - Stoppen na inzenden VE naar OM?
  - Wanneer on-line bevraging toepassen (BVI-IB, MEOS)?
  - Wordt er elders ook gevolgd / is het wel een politie taak?

Voorstel

- **Wat moeten we nooit volgen:**
  - Personen in verwijderde onderzoeken (Wpg art 14) (? mln)
  - Personen in de 15 oude BVH omgevingen (3 mln)
  - Personen uit oude HKS omgevingen daterend voor 01/01/2010 (2,5mln)
  - Andere systemen?
  - Overleden personen (0,3 mln)
- **Uitzoeken:**
  - Vervuiling in personenserver? Opschonen (Vreemdelingen?, internetaangifte) Meerdere persoonskaarten aan een persoon?

Inleiding
De politie neemt persoonsgegevens af van de BRP. Om deze actueel te houden heeft de politie abonnementen (afnemersindicaties) op eerder afgenomen gegevens.
De personenserver is voor de politie het koppelvlak naar de BRP. Iedere persoon, ongeacht de hoedanigheid, die in een bronsystemen zoals de BVH wordt vastgelegd kan een persoonskaart binnen de personenserver krijgen en daarmee een gelijktijdige afnemerindicatie binnen de BRP.
Er heeft overleg plaatsgevonden met de Rijksdienst voor Identiteitsgegevens (RvIG) over de omvang van het aantal afnemersindicaties.
Los van de imago schade voor de politie, gelden de principes van de Wpg ook voor het volgen van personen bij het GBA (proportionaliteit, doelbinding en subsidiariteit). Daarbij bestaat het risico dat de werklast sterk gaat toenemen voor de politie omdat met de Wet BRP de politie benaderd kan worden met de vraag waarom een persoon bevraagd is. Ook worden kosten in rekening gebracht voor het ontvangen van mutaties.

Uitgangspunten:
Iedere persoon waar de politie mee in aanraking komt zou in de personenserver moeten zitten maar het is niet nodig de actualiteit van iedere persoon hoog te houden, tenzij dit van belang is voor het politiewerk. Dit betekent dat functionaliteit nodig is in de personenserver waarmee een persoon, na verloop van tijd, niet meer automatisch wordt gevolgd in de Basisregistratie Personen.

Autorisaties op GBA en BRP
De politie heeft op dit moment 3 autorisaties op het GBA; Regulier, Gevoelig en Geheim. Voor deze drie autorisaties is een besluit gepubliceerd[1]. Bij de besluiten is opgenomen voor welk doel de afnemerindicatie geplaatst mag worden:

- Reguliere verstrekkingen: het verlenen van legitimatiebewijzen, vergunningen en ontheffingen.
- Gevoeilig: Indien het noodzakelijk is voor het uitvoeren van de politietaak, vreemdelingentoezicht of taken van de landelijke eenheden, zolang het verzoek gericht is op het verkrijgen van informatie over de ingeschrevene ten opzichte van wie de taken worden uitgevoerd. Het gaat hier vooral om Artikel 8,9 en 13 gegevens van de Wpg.
- Geheim: In het autorisatiebesluit staan dezelfde taken genoemd als onder “Gevoelig”. Het hier vooral om artikel 10 informatie van de Wpg.

Deze autorisaties zullen met de overgang naar BRP wijzigen. Zoals het er nu uitziet krijgt de politie twee autorisaties tot haar beschikking; “Geheim 1” dat overeenkomt met de geheime autorisatie en “Geheim 2”, dat overeenkomt met de reguliere en gevoelige autorisatie. Hierover is nog discussie gaande.

De volgende hoedanigheden waarin een persoon zich bevindt kunnen een afnemerindicatie krijgen.
Hierbij is niet rekening gehouden met de huidige situatie binnen de IV. Van een aantal personen, waarover de politie informatie vastlegt, is het noodzakelijk om mutaties te ontvangen ten behoeve van de handhavingstaak van de politie en ketenpartners binnen de openbare orde en veiligheidsdomein.

* Verdachten in lopende onderzoeken (in bvh dus afgehandeld="nee").

- Verdachten zijn een speciale doelgroep. Indien het hier gaat om artikel 8 Wpg informatie zal aangesloten moeten worden bij de verwerkingstermijn in de Wpg. In dit geval is dat 1 jaar na de eerste verwerking. De gegevens van de verdachte zijn voor infodeskmedewerkers tot vijf jaar beschikbaar en dat zou betekenen dat tot die tijd de afnemerindicatie actief is. Het gaat hier we l om verdachten, die ook daadwerkelijk als verdachte zijn aangemerkt en ingezonden zijn naar het OM.

[1] De autorisatie besluiten zijn gepubliceerd op de website van de RVIG: http://publicaties.rvig.nl/Besluiten_en_modelautorisaties/Besluiten/BRP_besluiten/Ministeries/Ministerie_van_Veiligheid_en_Justitie?pagenr=2

* Personen met een risicoclassificatie. Dit betreft gegevens uit het voormalige HKS en wordt gezien als artikel 13 Wpg informatie.
* Doelgroepen (in Amazone)
* Gesignaleerden, waaronder personen met een executieopdracht
* Twijfelachtig: Personen met een wapenvergunning. Het kan relevant zijn om een signaal te krijgen als de persoon met een wapenvergunning komt te overlijden. We hebben als politie een taak en het aantal is niet hoog. Daarmee is het niet vreemd om voor deze doelgroep een afnemerindicatie te plaatsen.
* Zeer twijfelachtig: Personen in de rol van getuige of aangever: Deze personen zou je ook opnieuw kunnen bevragen bij de BRP als je als politie wilt communiceren. Onlangs is een analyse uitgevoerd naar het effect van het soptzetten van het stopzetten van de afnemerindicaties op personen die alleen voorkomen in de oude BVH's. Daaruit bleek dat met slachtoffers, vanuit de politie, vooral via mail en telefoon contact wordt opgenomen.

Implicaties:

- Als een persoon overlijdt, hoeven we geen afnemerindicatie te hebben. Deze vervalt na 2 maanden (vanwege administratieve fouten waarop correcties kunnen plaatsvinden)
- De gebruiker moet kunnen zien wat de actualiteit is. De gebruiker moet kunnen zien wanneer de laatste synchronisatie met de basisregistratie heeft plaatsgevonden.
- Er zijn dus statuswijzigingen die aanleiding geven om de afnemerindicatie te verwijderen of te plaatsen (bijv hoedingheid of status registratie). Ook bij het schonen van persoonsgegevens, gelet op de Wpg-termijnen, zullen uiteraard ook de eventuele afnemerindicaties verwijderd moeten worden.
- Toets bij Gegevensgebruik en –beheer als er voorzieningen worden aangesloten op de Basiregistratie personen en de personenserver (of later kernregister personen)

Openstaande vragen

- Wat is de rol van politie tav Jeugd? In het verleden had de politie een belangrijke rol als het gaat om jeugd. Het gaat daarbij om contacten met school (zachte informatie) en signalen geweld binnenshuis (ZSM-jeugd, vroegsignaleren en doorverwijzen, Landelijke Instrumentarium Jeugd). Er is niet altijd sprake van een strafbaar feit maar de politie staat wel in de frontlinie. Vaak wil men ook de adresmutaties hebben van familie-leden/huisgenoten omwille van risico-taxatie en de betrouwbaarheid van de rapportage. De vraag hieraan vooraf gaat is; in hoeverre past dit binnen de politietaak en in hoeverre is dat proportioneel? Een vraag voor
- Personen die een gevaar vormen voor zichzelf en hun omgeving (5.1.2.e). Ook hier is het de politie die continu aanwezig is.
- Is er onderscheid aan te brengen in maatschappelijke classificaties of delicten? Voor sommige delicten misschien meerdere hoedanigheden volgen en langer volgen dan voor anderen?
- Wat is nu de omvang van de personen die we nu volgen, kijkend naar de hoedanigheden (waaronder jeugd)? Hoeveel verhuis- en status mutaties ontvangt de politie?

IV

- Voormalige HKS functionaliteit: Antecedenten en personen met een risico-classificatie zijn overgezet naar geconsolideerde BVH's. Het gaat hier om artikel 13 informatie. Voor artikel 8 informatie geldt dat de gegevens
- Worden de antecedenten na 5 jaar verwijderd in BVH? Hoe staat het met de schoning-scripts en worden de afnemer-indicaties verwijderd?
- Indien voor specifieke rollen de afnemer-indicaties worden hersteld in de oude BVH's, dienen dezelfde bedrijfsregels geïmplementeerd te worden in de eenheid BVH's.

0614

Basisobject register (BOR)

Besluiten en status

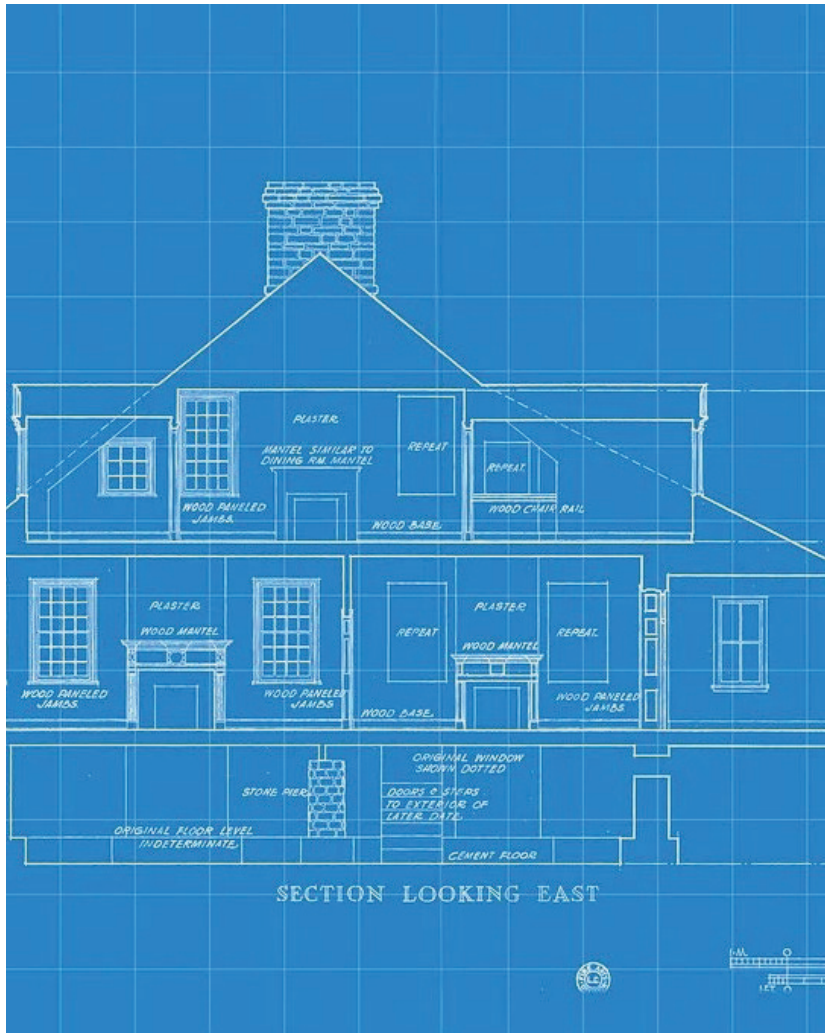
De basis is op orde we kunnen bouwen

Eenmalig vastleggen, meermalig gebruiken

POLITIE

We hebben de Blauwdruk

Het ontwerp van BOR Voertuig is toepasbaar voor alle BORren



Met deze basis zijn we in staat om:

- een gegevensobject (voertuig) registreren door:
  - Gegevens uit een authentieke bron te gebruiken
  - Handmatig op te voeren (als er geen authentieke bron)
- (handmatig) eigen politie gegevens vastleggen, ongeacht of er een authentieke bron is
- conflicterende gegevens uit verschillende bronnen op te slaan en weer te geven
- een reeds opgevoerd object (voertuig) hergebruiken o.b.v. een uniek ID over verschillende dossiers heen
- in de simpelste* vorm verwerken (inzien / vastleggen en bijwerken / verwijderen)
- gegevens op te slaan volgens de vereisten van de WPG, AVG en de archiefwetgeving
- Rekening houdend met PSbD
- d.m.v. een extra handeling historische data opvragen**

*Dit is het basisniveau in het volwassenheidsmodel (work in progress)

**I.v.m. gekozen database scheiding t.b.v. performance (CQRS; actuele stand en historie) is een platform aanpassing noodzakelijk

Wat komt er nog aan

- Het volwassenheidsmodel i.c.m. gewenste functionaliteit vanuit ringen bepalen welke vervolgstappen prioriteit krijgen, bijvoorbeeld:
  - Gebruik van de peildatum om historische gegevens uit de BOR op te halen
  - ...
  - “De stekkerdoos”; De BOR buiten RAPP beschikbaar stellen

Idem als de basis willen we dit in één keer generiek ontwerpen en beschikbaar maken voor alle BOR-en

PVR definitie BOR

Een BasisObjectRegister is een fysiek **register** waarmee alle voor de politie relevante **kenmerken** van één specifiek **gegevensobject** centraal worden beheerd en kan worden ontsloten voor **(her)gebruik*.**

*(her)gebruik: Het PVR compliance loket i.s.m. SEMA komt z.s.m. met een definitie.

Deze definitie is een samenstelling van de **vastgestelde** Basisobjectregister & Objectregister definities. De reden hiervoor is dat onderscheid, in zowel naamgeving als werking, het gewenste architectuureffect vermindert. Hiermee onderkennen we dus alleen nog maar BOR-en (geen OR o.i.d.).

Na overleg PMST, compliance en architectuur goedkeuring door 5.1.2.e (04-11-2022).

Zienswijze gegevensarchitectuur & SEMA

De gegevens die onder het beheer van een BOR vallen worden vaak verward met de gegevens die getoond (mogen) worden aan een gebruiker. Dit betekent dat de gebruiker **niet per definitie alle gegevens ziet** die in de BOR zijn opgenomen.

Wat je kan **zien** is onderdeel van het **gebruik** van de (RAPP-)functionaliteit. Dit staat feitelijk los van een BOR en is daarmee **niet bepalend voor welke** gegevens in één specifieke BOR horen.

Architectuur en SEMA adviseert welke gegevens in een BOR worden opgeslagen om (her)gebruik en beheer te BORgen.

Compliance adviseert wanneer het (her)gebruik van de gegevens is toegestaan (autorisaties).

Techniek adviseert **hoe** deze gegevens beschikbaar worden gesteld.

SPO besluit op basis van de afgegeven adviezen

Leidraad gegevensarchitectuur & SEMA

Uit externe registers (bijvoorbeeld uit het RDW) krijgen we meerdere soorten gegevens terug. Je legt een specifieke relatie tussen deze objecten vast als dat nodig is.

- over **voertuigen** → datum inschrijving, merk
- over **personen** → BSN van kentekenhouder
- over **bedrijven** → bedrijfsauto's, lease auto's
- over **processen** → verlopen APK, gestolen

Dit zijn verschillende gegevensobjecten:

een **voertuig** is **geen persoon** en een **persoon** is **geen bedrijf**

Eenmalige opslag en beheer door een BOR van de gegevens voor hergebruik:

Gegevens van een kentekenhouder moeten bij het juiste gegevensobject worden opgeslagen. Als deze persoonsgegevens (ook) bij de entiteit Voertuig worden vastgelegd staan ze niet alleen op de verkeerde plek maar wordt het ook nog eens twee keer opgeslagen en resulteert dit in dubbel beheer.

Dit gaat in tegen het principe van eenmalig opslaan en meervoudig gebruik en staat haaks op de zienswijze van architectuur.

Vanuit de Business bezien

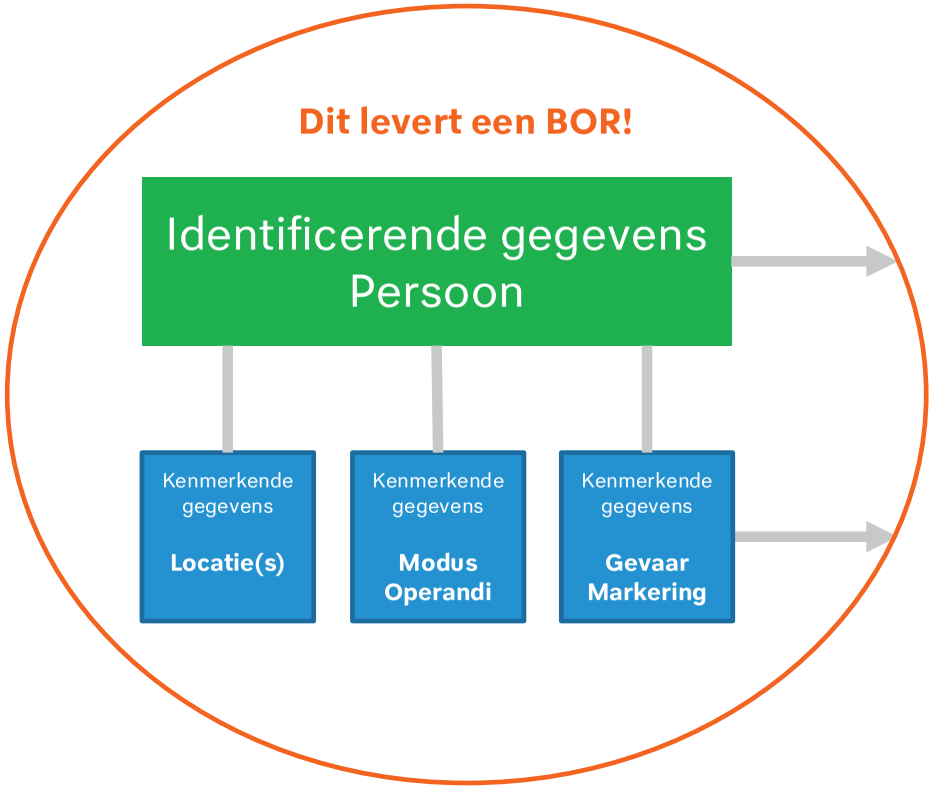
Kunnen al deze gegevens nodig zijn voor politiewerk.

- over **voertuigen** → klopt de kleur en merk en moet ik niet een onderzoek starten
- over **personen** → is de kentekenhouder wellicht “een bekende van” de politie
- over **bedrijven** → is dit bedrijf “een bekende van” de politie
- over **processen** → moeten we een voertuig in beslag nemen

Waarbij het (na besluit van diender) bij registratie belangrijk is dat:

- Kloppen de actuele gegevens die ik wil gebruiken met **de waarneming** van dat moment
- het **voertuig** eenvoudig moet kunnen worden vastgelegd
- een **bestuurder** eenvoudig moet kunnen worden vastgelegd
- …

Blauwdruk van Voertuig toegepast op Persoon



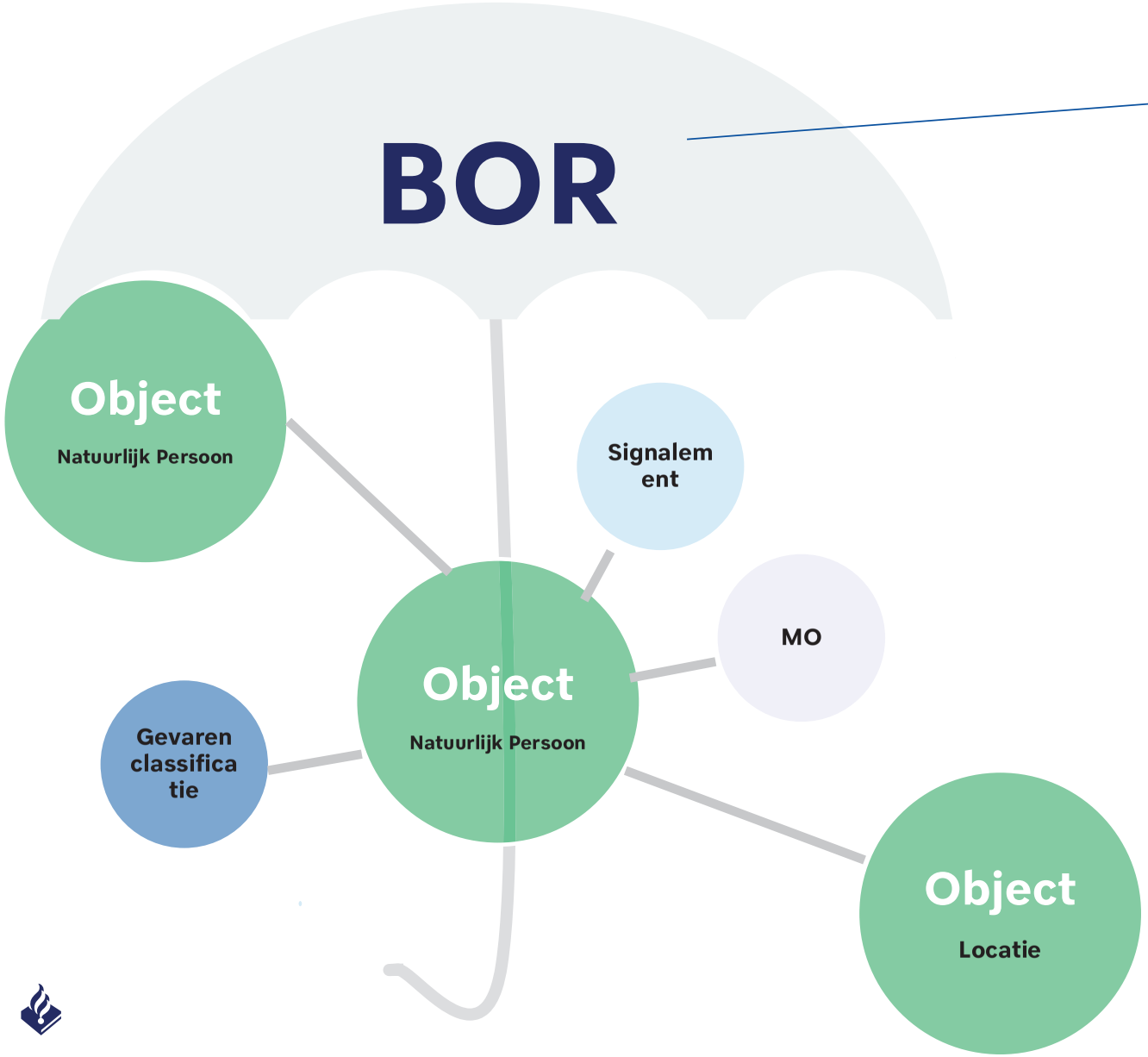
Dit zijn identificerende gegevens die de **kern** van een Persoon aangaan.

Deze gegevens hebben een sterk inhoudelijke relatie met de inhoud van een externe basisregistratie. (In dit geval het BRP). Waarbij het hebben van een (externe) bron optioneel is. Het gaat hierbij om gegevens waarmee iets of iemand uniek identificeerbaar is.

Dit zijn kenmerkende gegevens van een persoon en **zeggen iets over** een persoon

Vanuit de identificerende gegevens ligt een specifieke relatie naar de kenmerkende gegevens. Deze gegevens zijn zelfstandig inzetbaar volgens de definitie van een BOR.

Let op, we moeten veel meta gegevens vastleggen, noodzakelijk voor correct gebruik, waaronder verantwoording, autorisatie en de life cycle van de gegevens die ook van toepassing zijn voor de relaties. Dit zijn NFR's vanuit de autorisatiewerkgroep van toepassing op alle BOR-en



ZAAK

Identificerende gegevens van Persoon:

Dit zijn identificerende gegevens die de **kern** van een Persoon aangaan:

- Naam
- Geboortedatum
- (persoonsgebonden) nummer(s) / identificaties
- Geboorteplaats

Kenmerkende gegevens van een Persoon:

- De persoon heeft 0 of meerdere Signalementen
- De persoon heeft 0 of meerdere Modus Operandi
- De persoon heeft 0 of meerdere Gevarenclassificaties

Kan een relatie hebben met een andere identificerende gegevens (o.a.):

- De persoon heeft 0 of meerdere Adressen (locaties)
- De persoon heeft 0 of meerdere ouders / voogd (persoon)

Het is niet nieuw! DEMO Intel

- Bij de Intel wordt ook gebruik gemaakt van deelverzamelingen persoonsattributen die bij een hoofdverzameling persoon horen, gegevens zijn op basis van urgentie, samenhang en gebruikerslogica gepresenteerd


BVI Integraal Beeld
Identificerende gegevens
Kenmerkende gegevens
Welkom Annick Ranke
Startpagina > Zoek persoon > Persoonsbeeld
Persoon
Bluespot
BRP
BVH
BSN:
Achternaam:
Voorvoegsel:
Voornamen:
Geslacht:
Geboortedatum:
Geboren te:
Geboorteland: NEDERLAND
Nationaliteit: NEDERLANDSE
Niet onder reikwijdte
Gevarenclassificaties (12)
Bluespot
E&S
NL-SIS-II
Type Omschrijving Datum Gevalideerd
Harddruggebruiker ja
Verzetpleger ja
Alcoholist ja
Vluchtgevaarlijk ja
Hepatitis nee
Vuurwapengevaarlijk ja
Medische indicatie ja
Aandachtsvestigingen op persoon (19)
Bluespot
Startdatum Einddatum Titel
TOON MEER
Afspraken op locatie (4)
BVH
Startdatum Einddatum Adres
Locatie (1)
BRP
Adres Datum
Doelgroep (0)
AMAZONE
SUMMIT
Geen doelgroepen gevonden.
Signalering (0)
E&S
NL-SIS-II
Geen signaleringen en executieopdrachten gevonden.
Signalementen (25)
Bluespot
Signalement Datum
Voertuig (0)
RDW
Geen voertuigen gevonden.
Politie-antecedenten (225)
Bluespot
Categorie Omschrijving Datum
TOON MEER
Registraties (93)
SUMMIT
BVH
Omschrijving Rol Datum
TOON MEER

Interne memo

POLITIE

Organisatieonderdeel Staf korpsleiding/ Directie Informatievoorziening/ Gegevensautoriteit

Behandeld door 5.1.2.e
Functie Senior beleidsmedewerker
Telefoon 06 5.1.2.e
E-mail 5.1.2.e @politie.nl
Opgesteld in overleg met 5.1.2.e – 5.1.2.e BVH
Datum 26-07-2016
Versie 1.0 Vastgesteld op 20-7-2016 in het KMTO (zie paragraaf besluitvorming)

Onderwerp **Vernietigen politiegegevens in BVH**

Inleiding

Momenteel wordt er in BVH en BOSZ nog niet vernietigd conform de Wet politiegegevens (Wpg). In zijn brief aan de Tweede Kamer van 23-6-2014 heeft de Minister toegezegd dat we voor de twee grootste systemen (BVH en Summ-IT) maatregelen treffen om conform de Wpg te kunnen werken.[1] In de stuurgroep BVH is besloten dat ná ingebruikname van de release die functionaliteit bevat waarmee geautomatiseerd *verwijderd*[2] kan worden, functionaliteit wordt ontwikkeld om geautomatiseerd te vernietigen.

Dit memo beschrijft de uitgangspunten en het mechanisme hoe deze vernietiging plaats kan vinden. Deze worden verder uitgewerkt in een functioneel ontwerp. Het doel is zoveel mogelijk aan de Wpg te voldoen wat betreft het vernietigen van artikel 8-gegevens. Te vernietigen gegevens zijn met name algemene mutaties, meldingen, APV, parkeerboetes, verkeerscontroles, waarnemingen tijdens surveillance, et cetera. Hier worden geen processen-verbaal opgeslagen en alle gegevens kunnen na 10 jaar vernietigd worden.

Audit Wpg en verbeterplan

De in 2014 en 2015 uitgevoerde audit op de Wpg laat zien dat de politie op diverse fronten nog niet aan de wettelijke vereisten voldoet.[3] In het wettelijk verplichte verbeterplan wordt beschreven dat voor elke tekortkoming eerst gekeken wordt of ICT-maatregelen de risico's kunnen verkleinen. Alleen als dat niet mogelijk is, wordt er gekeken naar aanpassingen in de werkprocessen of opleidingstrajecten. De Wpg schrijft voor dat artikel 8-gegevens na vijf jaar verwijderd moeten worden en na tien jaar vernietigd moeten worden.

Uitgangspunten

Onderstaande uitgangspunten zijn bepalend voor hoe het algoritme voor het vernietigen eruit ziet:

1. BVH bevat voor het merendeel artikel 8-gegevens, maar eveneens artikel 9 en 13-gegevens.
2. Het is niet mogelijk gegevens in BVH geautomatiseerd als artikel 8-gegevens te herkennen (er is geen labeling). Dit is inherent aan de huidige functionaliteit in BVH.
3. Er wordt vernietigd op het niveau van registraties; dus een registratie wordt in haar geheel al dan niet vernietigd (hier kunnen dus meerdere voorvallen met verschillende maatschappelijke klassen onder vallen).
4. Zowel maatschappelijke klassen als de aanwezigheid van een (bepaald type) proces-verbaal, kunnen een indicatie zijn dat een registratie niet vernietigd wordt.
5. Wanneer artikel 13-gegevens (bijv. voormalige HKS-gegevens) herkend worden als zijnde artikel 13-gegevens, worden deze uitgesloten van het vernietigingsalgoritme.

---

[1] Lees de Kamerbrief over de evaluatie van de Wpg en de Wjsg.

[2] In het document uitgangspunten voor Wpg-schoning zijn de uitgangspunten en principes opgenomen hoe verwijdering plaatsvindt. Ook voor het verwijderen geldt dat dit mechanisme op zowel BVH als BOSZ van toepassing is.

[3] Lees de Kamerbrief naar aanleiding van de Wpg-audit en andere privacyonderzoeken.

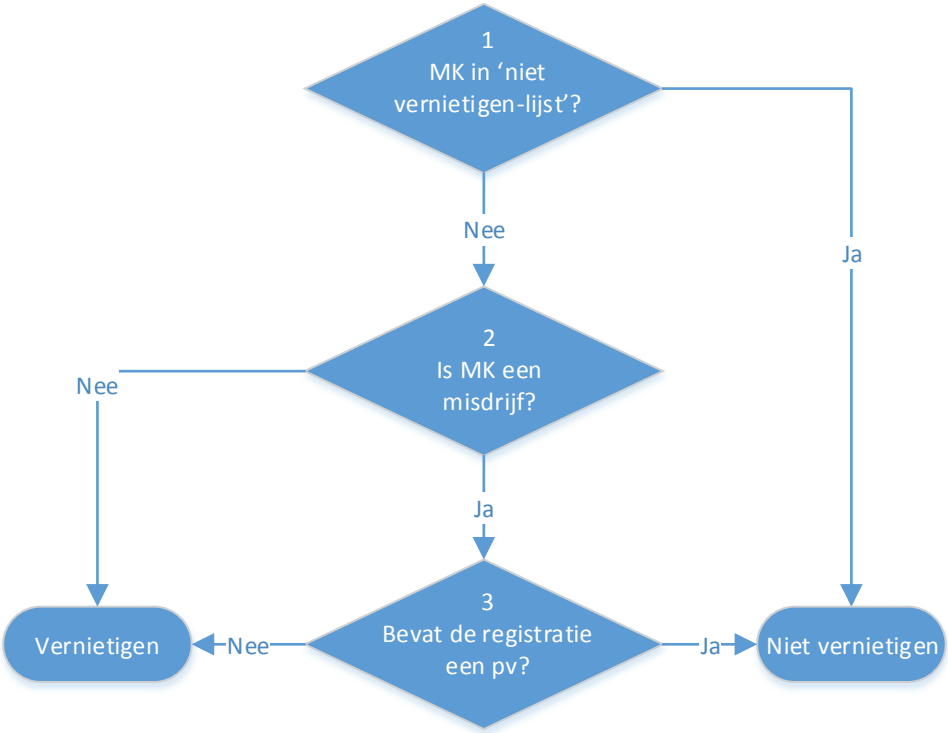
6. Landelijke werkprocessen rondom het gebruik van BVH zijn leidend. Oneigenlijk gebruik van BVH vormt mogelijk een risico voor het vernietigen.[4]
7. Alleen gegevens die “Wpg verwijderd” zijn, kunnen vernietigd worden. Lees ook het memo dat het verwijderingsmechanisme beschrijft.

Strategische beslissingen Chief Data Officer

1. Alleen gegevens die evident onder het artikel 8-regime vallen, worden vernietigd. Er wordt dus ‘voorzichtig’ vernietigd. Deze beslissing komt voort uit uitgangspunt één en twee.
2. De wijze waarop vernietigd wordt is zo eenvoudig mogelijk. Dit komt de onderhoudbaarheid en transparantie ten goede wat noodzakelijk is vanwege de vele koppelingen met andere informatiesystemen zoals BOSZ en BVI. Bij voorkeur is ook de technische uitwerking zo eenvoudig en transparant mogelijk.
3. Naast dit mechanisme dient er gewerkt te worden aan een oplossing om op middellange termijn BVH volledig Wpg-bestendig te laten zijn.

Mechanisme/ wijze van vernietiging

Selecteer alle registraties met een datum eerste vastlegging van 10 jaar of langer geleden met status ‘Wpg Verwijderd’.[5] Alles dat vernietigd wordt, krijgt dus eerst de status ‘Wpg verwijderd’.[6] De registratie kan worden vernietigd tenzij de beslisboom anders uitwijst. Niet alleen de registraties en voorvallen worden vernietigd, maar ook alle entiteiten (zoals personen, goederen, formulieren) die daaraan gekoppeld zijn en niet aan een andere registratie hangen, worden vernietigd.



1. Bevat de registratie ten minste één voorval met een **maatschappelijke klasse (MK)** opgenomen in de tabel in de bijlage? Zo ja, dan wordt de registratie niet vernietigd.
2. Bevat de registratie ten minste één voorval met een maatschappelijke klasse van het type “**misdrijf**”[7]? Zo ja, ga door naar stap 3.
3. Bevat de registratie een formulier dat een “**proces verbaal**“ is, zoals gekenmerkt in de tabel in de bijlage? Zo ja, dan wordt de registratie niet vernietigd.

[4] Bijvoorbeeld het inrichten van een doorlopende registratie voor verkeerscontroles en IGP-opdrachten wordt als oneigenlijk gebruik beschouwd. Hetzelfde geldt voor een DNA-afname: daar dient altijd een proces-verbaal bij aangemaakt te zijn.
[5] Een registratie krijgt deze status in principe als ze 5 jaar of ouder is. Zie de betreffende notitie.
[6] Dit hoeft niet te betekenen dat gegevens vijf jaar lang ‘verwijderd’ blijven voor ze vernietigd worden.
[7] Het betreft hier niet de landelijke BVI-definitie van een misdrijf, maar de misdrijfindicatie zoals in BVH gebruikt wordt.

Toelichting stap 1 beslisboom: uitzonderen op basis van MK?
Op basis van de MK's die in een registratie voorkomen, kan een grove schifting gemaakt worden of een registratie mogelijk artikel 9 of 13-gegevens bevat.
Toelichting stap 2 beslisboom: misdrijf of overtreding
Als een registratie niet uitgezonderd wordt van vernietiging op basis van de MK, dan is het van belang of het om een overtreding, actie of misdrijf gaat. Overtredingen en acties worden vernietigd, daarbij doet het niet ter zake of er al dan niet een proces verbaal is opgemaakt.
Toelichting stap 3 beslisboom: beoordeling misdrijven
Voor de misdrijven die niet op basis van MK vernietigd worden, is het van belang of er een proces verbaal aanwezig is. Hiervoor is gekeken naar de artikel 13-reglementen HKS/Processen Verbaal & Rapporten die beschrijven welke processen verbaal langer dan 10 jaar bewaard kunnen worden. Zie de bijlage voor de lijst met formulieren die conform artikel 13 als proces verbaal worden beschouwd en daarom uitgezonderd worden van vernietiging. I.v.m. verschillende werkwijzen uit het verleden is het voor een juiste antecedentbepaling noodzakelijk om ook te controleren of er een verdachte is. Als er dus geen pv aanwezig is conform de lijst uit de bijlage, maar er is wel een verdachte, dan wordt de registratie uitgezonderd van vernietiging.

Proces totstandkoming mechanisme en toetsing
Deze beschrijving is tot stand gekomen na bijeenkomsten met de werkgroep vernietigen op 21 september, 4 november en 30 november 2015 en 19 januari en 23 mei 2016. Leden: 5.1.2.e , 5.1.2.e , 5.1.2.e , 5.1.2.e , 5.1.2.e , 5.1.2.e , 5.1.2.e , 5.1.2.e , 5.1.2.e . Na vaststelling van dit vernietigingsmechanisme, zal het verder uitgewerkt worden in een functioneel ontwerp. Dit wordt ook door BVI getoetst.

Versie 01 getoetst door 5.1.2.e (aansluiting BOSZ), 5.1.2.e leden werkgroep vernietigen en het landelijk gebruikersoverleg BVH 5.1.2.e Paar kleine wijzigingen doorgevoerd nav feedback incl. afspraken over oplegnota.
Versie 02 getoetst bij het Privacyplatform, 5.1.2.e (Juridische Zaken) 5.1.2.e (IM 5.1.2.e BVH), 5.1.2.e 5.1.2.e (BVI moet er rekening mee houden). Aanpassingen nav commentaar JZ van korpsstaf en BVI, privacyplatform was akkoord.
Versie 03 t.b.v. toets door 5.1.2.e (Directie Operatien), IM liason Summ-IT/ BOSZ (voorkomen dat registraties vernietigd worden die daar nog wel bestaan). Ter toets voor DGpol. Vervolgens t.b.v. besluitvorming in MTDIM, MTDICT, MTCIO, MT Staf KL en BOO.
Versie 04 ter vaststelling voor het KMT. Aanvulling in stap 3 van de beslisboom aangebracht n.a.v. bericht van BVI i.v.m. antecedentbepaling en bijeenkomst met de werkgroep vernietigen.

Besluitvorming

20-07-2016	vaststelling door het KMTO.
17-06-2016	akkoord door BOO, doorgeleiding naar KMTO.
31-03-2016	MTCIO gaat akkoord en benadrukt dat de functionele specs goed moeten worden gedocumenteerd. Bij een maatschappelijk debat kan dan een goed functioneel ontwerp overlegd worden incl. verwijzing naar het besluitvormingstraject. Zo kan de politie verantwoorden waarom en via welke route gegevens vernietigd zijn.
02-03-2016	Voorstel positief ontvangen door het Privacyplatform.
04-02-2016	Het Landelijk GebruikersOverleg BVH is akkoord en benadrukt dat gegevens nu daadwerkelijk vernietigd worden. Hier s.v.p. nadrukkelijk aandacht voor vragen in oplegnota.

Bijlage 1: maatschappelijke klassen die niet vernietigd worden
Elk voorval in BVH heeft een maatschappelijke klasse (MK). Er zijn verschillende soorten MK's: delict gerelateerd (D), niet delict gerelateerd (N) of een actie (A). Bij een D-MK is er altijd sprake van een misdrijf of overtreding. Het merendeel van de N-MK's wordt vernietigd. Een deel van de N-MK's wordt uitgesloten van vernietiging, bijvoorbeeld *terreurdreiging*. Voor die groep geldt dat dit geen typische artikel 8-gegevens zijn. Ook de MK *gevarenclassificatie*, die valt onder het regime van 13, wordt uitgesloten van vernietiging op basis van de MK.

Voor MK's geldt dat deze in de loop van de tijd wijzigen. Er vervallen klassen maar er komen er ook bij. Er is dus rekening gehouden met alle maatschappelijke klassen die ooit geregistreerd zijn. Het script zal periodiek (bijvoorbeeld elke drie jaar) geactualiseerd moeten worden om MK's die na 2015 zijn geïntroduceerd te beoordelen.

sleutel	omschrijving	Soort MK
E10	SCHIETPARTIJ (ZONDER VERVOLG)	N
E11	VECHTPARTIJ (ZONDER VERVOLG)	N
E13	HUISELIJKE TWIST (ZONDER VERVOLG)	N
E15	STEEKPARTIJ (ZONDER VERVOLG)	N
E23	TERREURDREIGING	N
E45	GEVARENCLASSIFICATIE	A
E90	LIJK(VINDING) NIET NATUURLIJKE DOOD (GEEN MISDRIJF)	N
E91	LIJK(VINDING) ZELFDODING	N
E92	LIJK(VINDING) NATUURLIJKE DOOD	N
F14	BOMAANSLAG	D
F520	OPENBARE SCHENNIS DER EERBAARHEID	D
F521	VERKRACHTING	D
F522	AANRANDING	D
F523	OVERIGE ZEDENMISDRIJVEN	D
F524	VROUWENHANDEL/KINDERHANDEL	D
F525	PORNOGRAFIE	D
F526	INCEST/AFHANKELIJKHEID/WILSONBEKWAME	D
F527	SEKSUEEL MISBRUIK KINDEREN (GEEN INCEST)	D
F5291	KINDERPORNOGRAFIE	D
F5292	KINDERPROSTITUTIE	D
F5293	MENSENHANDEL	D
F5294	MENSENSMOKKEL	D
F540	DOODSLAG/MOORD	D
F541	EUTHANASIE	D
F542	OVERIGE MISDRIJVEN TEGEN HET LEVEN	D
F543	ILLEGALE ABORTUS	D
F551	ZWARE MISHANDELING	D
F71	HANDEL VUURWAPENS	D
F74	INBEWARING GEVEN WAPEN	N
H44	VERMISSING PERSOON	N
H441	VERMISSING MEERDERJARIG PERSOON	N
H442	VERMISSING MINDERJARIG PERSOON	N
I40	VERLENEN VERGUNNING / ONTHEFFING	A
I41	INTREKKEN VERGUNNING / ONTHEFFING	A
I42	ADVISEREN OVER VERGUNNING / ONTHEFFING	A
I43	WEIGEREN VERGUNNING / ONTHEFFING	A
L51	LUCHTVAARTONGEVAL MET GEWONDEN	N
L52	LUCHTVAARTONGEVAL MET DODEN	N
L53	LUCHTVAARTONGEVAL ZONDER GEWONDEN	N
L6	SPOORWEGONGEVALLEN	N

Bijlage 2: PV Formulieren

Als de registratie een voorval met de MK van het type “misdrijf” bevat en er een formulier aanwezig is dat een “proces verbaal” is, wordt de registratie niet vernietigd. Dit zijn alle formulieren met een sleutel die begint met de letters PV en de hieronder genoemde. Bij de voormalige korpsen bestonden ook regionale processen-verbaal. Omdat het een onevenredige inspanning is deze alle te beoordelen, worden ook deze uitgezonderd van vernietiging. Deze beginnen alle met PV.

sleutel	naam	begindatum	einddatum
BVAANHOW	BEVEL AANHOUDING BUITEN HETERDAAD OVERLEVERINGSWET	23-okt-07	
BVIVL	VERLENGING BEVEL TOT INVERZEKERINGSTELLING	02-jan-00	
BVIVS	BEVEL TOT INVERZEKERINGSTELLING	02-jan-00	
BVOPHIDE	BEVEL VERLENGING OPHOUDEN TER IDENTIFICATIE	02-jan-00	
BVUITBG	BEVEL TOT UITLEVERING EX ART. 126A SV	01-jan-09	30-sep-13
BYBLO	BIJLAGE BLOEDONDERZOEK	23-okt-07	
BYGKVL	BIJLAGE WEGGENOMEN GOEDEREN	02-jan-00	
BYGOO	BIJLAGE OPSPORINGSGEGEVENS	02-jan-00	
BYKLN	BIJLAGE VERBALISANTEN	23-okt-07	
DOSSIER	MODELDOSSIER	02-jan-00	
FO8ARTS	VERSLAG VAN ARTS	02-jan-00	
FOACOMPO	FORMULIER AANVRAAG COMPOSITIEFOTO	01-sep-14	
FOACONFR	FORMULIER AANVRAAG CONFRONTATIE	01-sep-14	
FOBOB	FORMULIER BIJZ OPS BEV	02-jan-00	
FODNAISV	INSTEMMING TOT DNA ONDERZOEK	02-jan-00	
FODNATSV	TOESTEMMING DNA-ONDERZOEK	02-jan-00	
FOTOBLAD	FOTOBLAD	23-okt-07	
KVI	KENNISGEVING VAN INBESLAGNEMING	01-mrt-11	
MABINTR	MACHTIGING BINNENTREDEN	02-jan-00	
MILKORT	VERKORT MILIEU PV	01-jan-09	01-jan-09
SUMMIER	SUMMIER PROCES-VERBAAL	02-jan-00	
TRACOWAT	PV TRANSPORTCONTROLE WATER	01-mrt-14	
ZEEVACO	PV VAN BEVINDIGEN ZEEVAARTCONTROLE	01-apr-14	

POLITIE

Memo

Afzender
Portefeuille Intelligence, 5.1.2.e
Typ E-mailadres afzender
Typ Telefoonnr. afzender

Ontvanger(s)
Aan: Directie Operatiën, 5.1.2.e

Rubricering
Kies een item uit de lijst

Datum	15 april 2023	**Behandeld door**	Landelijk Portefeuilleteam intelligence
Ons kenmerk	Typ Ons kenmerk	**Kopie aan**	Typ Kopie aan
Uw kenmerk	Typ Uw kenmerk	**Bijlage(n)**	Typ Aantal bijlagen (getal)

Onderwerp Bevindingen politie m.b.t. BRP n.a.v. Investico onderzoek

Typ Aanhef,

Aanleiding

In maart 2023 verschenen in diverse landelijke media artikelen met koppen als: “Politie verzamelt op grote schaal data van demonstranten”. Uit bevindingen van Onderzoeksplatform Investico zou blijken dat de politie met grote regelmaat persoonsgegevens opvraagt, zoals hun adres, burger-servicenummer en geboortedatum. Daarnaast zou de politie gegevens van ouders en kinderen van actievoerders opvragen. Dit zou onder meer blijken uit 67 dossiers van demonstranten, die Investico, heeft onderzocht. De onderzochte gegevens zijn afkomstig uit de Basisregistratie Personen (BRP), een database waarin persoonsinformatie is opgenomen over iedere inwoner van Nederland.
Door gebruik te maken van een wettelijk inzagerecht kregen belanghebbenden inzicht door wie zij zijn bevraagd. De 67 dossiers hebben betrekking op demonstranten uit de antiracisme- en klimaatbeweging, waaronder Extinction Rebellion (XR), maar ook op corona-demonstranten en antifascisten die meededen aan het onderzoek van Investico. Uit de verkregen overzichten zou ook blijken dat gegevens van familieleden van nooit veroordeelde demonstranten worden opgehaald. Een landelijk bekende coronademonstrant zou in twee jaar tijd 1400 keer zijn bevraagd.

In de media-artikelen is de reactie van de politie verwoord. De taakstelling die de politie heeft bij het handhaven van de openbare orde, in het bijzonder bij demonstraties, wordt toegelicht. Hierin past volgens de politie dat persoonsgegevens worden opgevraagd. De politie kan echter geen logische verklaring geven waarom familieleden op uitgebreide schaal worden bevraagd in het BRP en waarom bijvoorbeeld iemand 1400 keer wordt bevraagd. Experts worden geciteerd, die aangeven dat door de ‘datahonger’ van de politie het recht op betoging in het geding is.

Kamervragen, raadsvragen en WOO-verzoeken

Naar aanleiding van de publicaties zijn inmiddels Kamervragen gesteld, evenals raadsvragen in de gemeenten Utrecht, Amsterdam en Den Haag. Ook zijn hierover diverse WOO-verzoeken bij de politie ingediend.

In de beantwoording op de Kamervragen wordt de taakstelling van de politie toegelicht:

“De politie heeft op grond van artikel 3 van de Politiewet 2012 tot taak in ondergeschiktheid aan het bevoegd gezag en in overeenstemming met de geldende rechtsregels te zorgen voor de daadwerkelijke handhaving van de rechtsorde en het verlenen van hulp aan hen die deze behoeven. Daarvoor heeft de politie gegevens nodig. De politie heeft informatie nodig om demonstraties te faciliteren en in goede banen te leiden en zo de veiligheid van demonstranten en omstanders te waarborgen, als uitvoering van de taak om de openbare orde te handhaven. Om zich goed op een demonstratie voor te bereiden kijkt de politie onder andere naar het aantal te verwachten demonstranten, op welke plek de demonstratie is, hoe de demonstratie van de betreffende organisatie de vorige keer verliep en hoeveel mensen er de vorige keer aanwezig waren. De politie voert gesprekken met de organisatoren van demonstraties en andere betrokkenen. Tevens beoordeelt de politie signalen van mogelijke tegendemonstraties/verstorende acties. Zo kan worden ingeschat hoeveel politie-inzet noodzakelijk is en kunnen de benodigde voorbereidingen en maatregelen worden getroffen voor een soepel en veilig verloop van de demonstratie. In dit kader worden persoonsgegevens verwerkt. Deze worden opgevraagd vanuit de Basisregistratie Personen (BRP) zodat actuele en correcte persoonsgegeven worden opgenomen in de politiesystemen. Artikel 4 (lid 1) van de Wet politiegegevens bepaalt dat de politie maatregelen moet treffen om de persoonsgegevens die zij verwerkt, juist en nauwkeurig te houden. In de Wet Basisregistratie personen (artikel 3.2 Wet Brp) en het op die wetgeving gebaseerde autorisatiebesluit BRP voor de politie is te lezen voor welke doelen en onder welke voorwaarden de politie de gegevens uit de BRP kan verkrijgen.”

Deze eerste reactie kan echter het grote aantal BRP-hits in het geschetste dossier van Investico niet verklaren.

Autorisatiebesluit BRP

De politie mag op basis van het autorisatiebesluit BRP, afgegeven door de Rijksdienst voor Identiteitsgegevens van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, ten behoeve van haar taakstelling persoonsgegevens opvragen. Met de door de politie gebruikte verwerkings- en bevragingssystemen kan het BRP geautomatiseerd worden benaderd. Hierbij gelden twee zogenaamde afnemersindicaties, waarbij één afnemersindicatie op geheim staat (zie art. 42, onder c, Besluit BRP). Geheime bevragingen gelden voor verwerkingen ten behoeve van onderzoeken in relatie tot art. 9 en 10 Wpg en kunnen slechts worden gedaan door specifieke politieonderdelen. De andere afnemersindicatie geldt voor de bevragingen ten behoeve van de algemene dagelijkse politietaak (art. 8 Wpg). Hierin worden door de politie de meeste bevragingen gedaan. Het onderzoek van Investico ziet op de bevragingen in het kader van deze dagelijkse politietaak.

Onderzoek bevragingen

Een werkgroep, onder leiding van de programmadirecteur intelligence, heeft nader onderzoek ingesteld naar de achtergronden van de bevragingen. De werkgroep bestaat uit vertegenwoordigers van diverse politieonderdelen (techniek, uitvoering, juridisch en integriteit).

De werkgroep richt zich op 4 vragen:

1. Waarom bevraagt de politie demonstranten?
2. Waarom doet de politie dat zo vaak?
3. Waarom bevraagt de politie ook ouders en kinderen?
4. Wat doet de politie met opgevraagde informatie?

Ad. 1. Waarom bevraagt de politie demonstranten?
De bevragingen richten zich niet op demonstranten in het algemeen, maar op personen die zich tijdens een demonstratie/betoging niet aan de voorschriften houden, strafbare feiten plegen of zich mogelijk schuldig maken aan (ernstige) verstoringen van de openbare orde. Dat kan resulteren in

aanhoudingen, staande houdingen en identiteitscontroles. Daarnaast worden in de aanloop naar demonstraties bevragingen gedaan naar de initiatiefnemers en ambtshalve bekende personen die mogelijk politiële aandacht vragen bij demonstraties, om een inschatting te kunnen maken van de risico's voor verstoringen van de openbare orde. Dit past allemaal binnen de taakstelling van de politie. Hiervoor geldt een open bevragingsregiem voor de algemene dagelijkse politietaak (art. 8 Wpg). De bevragingen hiervan worden zichtbaar in de BRP-tellingen.

Ad 2. Waarom doet de politie dat zo vaak?
De bevragingen van persoonsgegevens geschieden in de meeste gevallen via de systeemapplicaties Integrale Bevraging (IB) en het Integraal Persoonsbeeld (IP). Opgevraagde gegevens kunnen bijvoorbeeld worden getoond in een mobiel device op straat (smartphone)[1]. IB en IP fungeren als een schil naar uiteenlopende onderliggende bronregistraties, waarin de feitelijke verwerkingen van persoonsgegevens plaatsvinden. Deze bronregistraties, waartoe ook de registratie 'GBA' (toegang tot BRP) behoort, kunnen separaat uit- en aangezet worden. Omdat in het dagelijks politiewerk het BRP veel gebruikt wordt, staat deze bron bij de meeste politiemedewerkers standaard aan. Dat betekent dat al deze registraties worden doorzocht als er een bevraging via de schilapplicatie plaatsvindt. Een zoekslag om te bepalen of iemand eerder een strafbaar feit heeft gepleegd, zal dus vaak ook resulteren in bevragingen van het BRP.

Uit nader onderzoek blijkt dat elke bevraging van een persoon veelal minimaal twee bevragingen van het BRP oplevert. De eerste bevraging toont een eerste selectie van hits, waarbij slechts naam en geboortedatum getoond worden. Als de bevrager vervolgens kiest om een detailbevraging te doen worden de volledige NAW-gegevens (naam, adres en woonplaats) aangeleverd. Dit levert bij een inzageverzoek van een burger een dubbeltelling op. Met dit algemene gegeven dient het aantal bevragingen op persoon op voorhand met de helft te worden gereduceerd. Het gaat hierbij dus om een technische oorzaak.

De bevragingssystemen werken zo dat wanneer er teruggeklikt wordt naar de zoekresultaten en opnieuw op 'toon details' wordt gedrukt dit wederom een bevraging van de BRP veroorzaakt. Daarnaast zijn eerder gedane zoekvragen (zoekgeschiedenis) zichtbaar en ook als daar op geklikt wordt zal dit leiden tot wederom een bevraging van het BRP. Het systeem slaat eerder verkregen resultaten dus niet op maar bevraagt de onderliggende bronnen iedere keer opnieuw. Dit kan leiden tot meerdere bevragingen van het BRP.

Als er bij briefings, als toelichting op de operationele inzet tijdens en context van demonstraties, specifiek op bepaalde personen (mogelijke ordeverstoorders) wordt gewezen, zoeken medewerkers de gegevens over deze personen regelmatig terug via IB. Deze acties zijn verklaarbaar vanuit de taakstelling en ondersteunen de operationele inzet. Tegelijkertijd vertekenen deze bevragingen het beeld bij inzageverzoeken in het BRP.

Als een persoon wordt aangehouden worden diens gegevens ingevoerd in de bronregistratie BVH. Bij de invoer kunnen er ook bevragingen van de BRP gedaan worden om ervoor te zorgen dat de gegevens juist in de BVH worden ingevoerd. Daarnaast wordt er automatisch een 'abonnement' gegenereerd bij het BRP. Dat betekent dat bijvoorbeeld adreswijzigingen automatisch worden doorgegeven aan de politie. Dat garandeert de integriteit van de vastgelegde informatie en voorkomt eventuele fouten in latere operationele afwegingen. Deze abonnementen leiden overigens niet tot de aanname dat dit grote invloed heeft op de omvang van individuele persoonsbevragingen.

Ad 3. Waarom bevraagt de politie ook ouders en kinderen?
Bij een detailbevraging van een persoon in het BRP wordt een aantal basisgegevens van de ouders en kinderen van die persoon automatisch meegegeven. Het gaat dan om BSN, naam, geslacht en geboortedatum. Ouders en kinderen worden dus niet apart of volledig bevraagd en er is volgens het BRP ook geen bevraging van die ouders en kinderen gedaan. Het zijn gegevens die bij een persoon

[1] Op de smartphone zit de tool 'mobiel effectief op straat'(MEOS), waarmee op elk moment en elke plaats informatie kan worden opgevraagd.

horen net zoals een adres. Iedere detailbevraging die de politie doet bevat dus deze gegevens. Dit is niet aanpasbaar door de politiemedewerker. Deze familiegegevens verschijnen echter niet standaard in het detailscherm dat de politiemedewerker getoond krijgt. Hiervoor moet een aantal handelingen worden verricht. Voor het zicht krijgen op een openbare ordeverstoring is er geen reden om deze gegevens te bekijken.

De politie bevraagt dus niet apart ouders en kinderen maar krijgt een klein aantal gegevens van ouders en kinderen mee met de bevraging van iedere persoon in het BRP.

Ad 4. Wat doet de politie met opgevraagde informatie?
Veelal is de bevraagde informatie benodigd om een goed beeld te krijgen van een situatie. Het draagt bij aan het maken van inschattingen vooraf, het opstellen van veiligheidsbeelden of aan de beoordeling van een situatie ter plaatse, waarmee de politieambtenaar wordt geconfronteerd. De bevraging kan de start vormen voor het daadwerkelijk vastleggen van informatie in de politiesystemen. Niet elke bevraging leidt echter tot vastlegging. Dit zal afhangen van hoe de politieambtenaar de bevraagde informatie beoordeelt op relevantie voor de taakstelling. Hierin bestaat ruimte voor een professionele afweging.