POLITIE

Memo

Afzender
5.1.2.e
5.1.2.e @politie.nl
06 5.1.2.e
Programma intensivering privacy
Deelproject Registerplicht & GEB

Ontvanger(s)
Portefeuillehouder Specialistische Opsporing

Rubricering
Politie INTERN – Bedrijfsvoering

Datum	22 december 2023	**Behandeld door**	5.1.2.e
Ons kenmerk	20231113-01	**Kopie aan**	Typ Kopie aan
Uw kenmerk	Typ Uw kenmerk	**Bijlage(n)**	1

Onderwerp Addendum GEB "Biometrievoorziening HAVANK 4 & CATCH 2" m.b.t. Dactyloscopie

Basisinformatie

Naam van de verwerking zoals aangemeld in 5.1.2.I	Dactyloscopie
Ingangsdatum van de verwerking	Bestaande verwerking
Gemandateerd verwerkingsverantwoordelijk Portefeuillehouder en eenheid	Wilbert Paulissen (W.J.A.), Eenheid Oost-Brabant
Politieonderdeel waar de verwerking plaatsvindt	Landelijke Eenheid
Contactpersoon m.b.t. deze verwerking	5.1.2.e
Privacyfunctionaris	5.1.2.e / 5.1.2.e

Betrokken bij deze GEB	**Naam**
Privacy adviseur programma	5.1.2.e , 5.1.2.e @politie.nl (06 5.1.2.e)
Reviewrol privacy adviseur programma	5.1.2.e
IB Analist programma	5.1.2.e
Privacyfunctionaris portefeuille	5.1.2.e
Adviseur portefeuillehouder	5.1.2.e
Senior business expert	5.1.2.e

Functionarissen gegevensbescherming	5.1.2.e / 5.1.2.e
Advies FG nodig: ja/nee	Wanneer advies noodzakelijk is als bijlage toevoegen
Datum	<invullen>
Toelichting: Er is invulling gegeven aan de adviesrol van de functionaris gegevensbescherming door uitvoering van een externe review door de privacyfunctionaris van Oost-Brabant, tevens privacyfunctionaris van de portefeuille Specialistische Opsporing.	

Gezien door verwerkingsverantwoordelijke

Naam	Wilbert Paulissen
Functie	Korpschef (OS) – Hoofdcommissaris
Datum	<invullen>
Opmerkingen	

Addendum GEB Biometrievoorziening HAVANK4 & CATCH2 m.b.t. dactyloscopie

Introductie en scope

Dit document is een aanvulling op de GEB Biometrievoorzienig HAVANK4 & CATCH2 (hierna: GEB Biometrievoorziening) en vormt, samen met de GEB Biometrievoorziening de GEB op de verwerking “Dactyloscopie”. De processen gerelateerd aan gelaatsherkenning, die gerelateerd zijn aan CATCH2 en onderdeel zijn van de GEB Biometrievoorziening, zijn geen onderdeel van dit document maar zijn in een ander addendum beschreven.[1]

Dit document heeft als doel om de informatie over de verwerking van politiegegevens bij de vergelijking van vingerafdrukken, zoals beschreven in de GEB Biometrievoorziening, aan te vullen. Deze aanvulling heeft als basis het model GEB van het programma intensivering privacy, meer specifiek het deelproject “Registerplicht & GEB” (hierna: het deelprogramma). De aanvulling op de GEB Biometrievoorziening is noodzakelijk om aan de voor het deelprogramma geldende standaard te voldoen. De GEB Biometrievoorziening voorziet slechts ten dele in de volledige behoefte van het deelprogramma omdat de GEB geschreven is vanuit het perspectief van de HAVANK4 en CATCH2-applicaties. Het deelprogramma benadert verwerkingen echter vanuit het perspectief van de bedrijfsprocessen, waarbij meerdere processen een verwerking kunnen vormen of een deel van een enkel proces een verwerking kan vormen. Waar naar het inzien van het deelproject lacunes bestaan zullen deze worden aangevuld in onderhavig addendum.

De volgende aanvullingen op de GEB Biometrievoorziening zijn nodig:

- Verantwoording van de argumenten voor het maken van een GEB op de verwerking dactyloscopie.
- Procesbeschrijving inclusief verwijzing naar het bedrijfsreferentiemodel.
- Informatie over de schaal en reikwijdte van de verwerking.
- Overzicht van autorisaties.
- Verantwoording gebruik bijzondere persoonsgegevens.
- Beoordeling van de proportionaliteit en subsidiariteit.
- Wettelijke verwerkingstermijnen.
- Beoordeling van verstrekkingen aan buitenlandse opsporingsdiensten.
- Privacy risico’s dactyloscopie.

Risiconiveau van de verwerking

Op grond van art. 4c Wet politiegegevens (hierna: Wpg) voert de verwerkingsverantwoordelijke een gegevensbeschermingseffectbeoordeling (hierna: GEB) uit op een verwerking indien er een hoog risico voor de rechten en vrijheden van de betrokkenen ontstaat bij die verwerking van politiegegevens.

[1] Zie 20231026 Addendum HAVANK 4 CATCH 2 v1.0.

Bij de beoordeling van de omvang van het risico vormt het besluit van de Autoriteit Persoonsgegevens (hierna: AP) inzake verwerkingen met een hoog risico een leidraad.[2] Dit besluit is gebaseerd op een publicatie van de voorganger van de EDPB, de art. 29 werkgroep.[3] Hoewel het besluit formeel uitsluitend toepasselijk is binnen het regime van de Algemene Verordening Gegevensbescherming (hierna: AVG) blijft het, volgens het deelprogramma, een geschikte leidraad om in eerste instantie een risico-inschatting mee te maken.

In het besluit van de AP staat een lijst met negen criteria. Als er aan twee (of meer) van deze criteria voldaan wordt spreekt men van een verwerking met een hoog risico voor de rechten en vrijheden van betrokkenen. De verwerking dactyloscopie voldoet in ieder geval aan de volgende criteria:

- Verwerking van gegevens van gevoelige of bijzondere aard. (4)
- Op grote schaal verwerkte gegevens. (5)

In de processen omtrent dactyloscopie wordt gebruik gemaakt van biometrische gegevens, namelijk vingerafdrukken. Biometrische gegevens zijn een van de categorieën bijzondere politiegegevens.[4] De biometrische gegevens zijn opgenomen in twee grote databanken waarvan één van deze databanken onder de verwerkingsverantwoordelijkheid van de Politie valt.[5] Deze databank met biometrische gegevens bevat de gegevens van ongeveer 2 miljoen betrokkenen, dit resulteert in een verwerking op grote schaal. Zowel het aanhouden van de databank als het vergelijkend doorzoeken van de databank vormen verwerkingsactiviteiten die samen in ieder geval tot een grootschalige verwerking van politiegegevens leiden.

Nu in ieder geval twee van de negen criteria vervuld zijn gaat er van de verwerking dactyloscopie een hoog risico voor de rechten en vrijheden van betrokkenen uit en is het derhalve noodzakelijk om een GEB uit te voeren op de verwerking.

Procesbeschrijving en bedrijfsreferentiemodel

Ter aanvulling van de procesbeschrijving in de GEB Biometrievoorziening een kort overzicht van de processen die onder de verwerking dactyloscopie vallen. De volgende processen zijn afkomstig van het Bedrijfsreferentiemodel (hierna: BRM).

Processen BRM:

- Vastleggen dactysignalement
- Afnemen sporen beslagene goed
- Beheren sporen
- Uitvoeren meervoudige procedure analyseren dactysporen
- Uitvoeren dactyloscopisch identiteitsonderzoek
- Verwerken resultaten onderzoek dactyspoor
- Maken dossier FO

[2] Besluit inzake lijst van verwerkingen van persoonsgegevens waarvoor een gegevensbeschermingseffectbeoordeling (DPIA) verplicht is , Autoriteit Persoonsgegevens.
[3] WP Art. 29, 4 oktober 2017, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679.
[4] Art. 5 Wet politiegegevens.
[5] Genaamd: HAVANK-strafrechtdatabase en HAVANK-vreemdelingendatabase.

Historie en context van de verwerking

Sinds 1989 bestaat de mogelijkheid tot geautomatiseerde vingerafdrukvergelijking. In datzelfde jaar werd de geautomatiseerde landelijke database Het Automatisch Vinger Afdrukkensysteem Nederlandse Kollektie (hierna: HAVANK) opgezet waarbij referentiemateriaal, vingerafdrukken van verdachten en veroordeelden, werd ingebracht. De databank met materiaal van verdachten en veroordeelden staat binnen de Politie bekend als de HAVANK-strafrechtdatabase. HAVANK is een applicatie ontwikkeld door het Frans/Amerikaanse Idemia welke op basis van met kunstmatige intelligentie ontwikkelde modellen en algoritmen vingerafdrukken, handafdrukken en voetafdrukken kan vergelijken.

Met de komst van de BVID-zuil (Basis Voorziening Identiteitsvaststelling) zijn de vingerafdrukken van de BVID-zuil de bron geworden voor het referentiemateriaal in de HAVANK-strafrechtdatabase. Elke keer als een betrokkene door middel van de BVID-zuil vastgelegd wordt en in de HAVANK-strafrechtdatabase blijkt te staan wordt de tijdens de registratie gemaakte vingerafdrukken aan de gecontroleerde persoon gekoppeld. Dit betekent dat de biometrische gegevens zoals deze bij de BVID-zuil worden verzameld in de database als referentiemateriaal worden gekoppeld aan de betrokkene door middel van de biometrie met een biometrienummer. Meer BVID-zuil controles resulteert voor de betrokkene in een grotere hoeveelheid gekoppeld referentiemateriaal aan zijn biometrienummer.

Er is ook een database met persoonsgegevens met vingerafdrukken van vreemdelingen. Deze database, Gezamenlijke Biometrie Voorziening (GBV)-vreemdelingendatabase genoemd, valt buiten de verwerkingsverantwoordelijkheid van de Politie. De GBV-vreemdelingendatabase is onderdeel van de vreemdelingen-administratie en valt onder de verwerkingsverantwoordelijkheid van de minister van Justitie en Veiligheid en volgt uit art. 107 lid 1 Vreemdelingenwet jo art. 106a Vw. Op de GBV-vreemdelingendatabase is de AVG van toepassing en niet de Wpg.

De GBV-vreemdelingendatabase wordt door de Politie gehost. De Politie is hierbij een verwerker in de zin van de AVG. De GBV-vreemdelingendatabase kan geautomatiseerd worden doorzocht op vordering van de officier van justitie met een machtiging van de RC .[6] Het onderzoek aan de GBV-vreemdelingendatabase wordt door de Politie uitgevoerd als verwerker zodat de verwerkingsverantwoordelijke (de minister van Justitie en Veiligheid) aan de vordering van de officier van justitie kan voldoen. Het geautomatiseerde onderzoek aan de GBV-vreemdelingendatabase valt buiten de verwerkingsverantwoordelijkheid van de Politie en daarmee ook buiten de scope van dit addendum en de GEB-biometrievoorziening.

Inhoud HAVANK-strafrechtdatabase

De HAVANK-strafrechtdatabase is een database met verschillende dactyloscopische kenmerken welke al dan niet gekoppeld zijn aan personen door middel van biometrienummers. De dactyloscopische kenmerken worden in de HAVANK-databases door middel van rekenkundige modellen omgezet in biometrische gegevens die geschikt zijn voor geautomatiseerde vergelijking. In de HAVANK-strafrechtdatabase kunnen de volgende sporen worden opgenomen:

- TP, *ten print*, de tien vingerafdrukken van één geïdentificeerd persoon. Deze sporen worden via de BVID-zuil opgehaald van aangehouden verdachten en aan de verdachte gekoppeld toegevoegd aan de database op grond van art. 55c lid 2 Sv.
- PP, *palm print*, de handpalmafdrukken van één geïdentificeerd persoon. Deze sporen kunnen op vordering van de officier van justitie worden verkregen op grond van art. 61a lid 1 sub b Sv. De handpalmafdruk van de verdachte wordt net als bij de TP aan de verdachte gekoppeld toegevoegd aan de database.

[6] Op grond van art. 126nf Wetboek van Strafvordering.

- LT, *latent fingerprint*, een (deel van een) vingerafdruk welke is veiliggesteld op een plaats delict of anderszins in het kader van een opsporingsonderzoek is veiliggesteld.
- LP, *latent palm print*, een (deel van een) palmafdruk welke is veiliggesteld op een plaats delict of anderszins in het kader van een opsporingsonderzoek is veiliggesteld.
- UL, *unsolved latent fingerprint*, een (deel van een) vingerafdruk welke is veiliggesteld op een plaats delict of anderszins in het kader van een opsporingsonderzoek is veiliggesteld waarbij geen verdachte in beeld is. Doorgaans in de context van een verzameling van onopgeloste vingerafdruksporen.
- ULP, *unsolved latent palmprint*, een (deel van een) palmprint welke is veiliggesteld op een plaats delict of anderszins in het kader van een opsporingsonderzoek is veiliggesteld waarbij geen verdachte in beeld is. Doorgaans in de context van een verzameling van onopgeloste palmafdruksporen.
- Footprint, afdruk van de blote voet met het papilairlijnenbeeld.
- ULFP, unsolved latent footprint, een deel van een blote voetafdruk die is veiliggesteld op een plaats delict etc.

De sporen naast LT en LP worden in de database vergeleken en, bij positieve individualisatie, aan een persoon gekoppeld door middel van het eerder geregistreerde Spoor *Identificatie Nummer* (SIN). Deze sporen worden niet gebruikt voor identificatie van een betrokkene bij een BVID-zuil. De BVID-zuil vergelijkt uitsluitend met TP-sporen.

Als positieve identificatie niet plaatsvindt komt het spoor als ongeïdentificeerd in de database te staan.

Procesflow
Het proces begint met een intake bij het centrale ontvangstloket van de Forensische Opsporing in de regionale eenheid. Er wordt onderscheid gemaakt in twee soorten onderzoek, de zogenaamde één-op-één vergelijking en de 1:n-vergelijking.

1:n-vergelijking

Met de 1:n-vergelijking levert de aanvrager sporen (LT, LP, UL of ULP) van een nog onbekende betrokkene aan die vervolgens eerst geautomatiseerd met de bestaande database met sporen vergeleken wordt. Het doel is om de identiteit van de betrokkene te achterhalen. Vergelijking vindt in ieder geval plaats in de HAVANK-strafrechtdatabase, indien er indicaties zijn dat de betrokkene een vreemdeling is wordt ook in de GBV-vreemdelingendatabase gezocht op vordering van de officier van justitie en met machtiging van de RC.

Het 1:n-onderzoek in de databases levert een match of no-match op. Een no-match wordt teruggekoppeld aan de aanvrager. De aangeleverde sporen blijven in de database staan als ongeïdentificeerd spoor. Bij een match worden de resultaten van de geautomatiseerde vergelijking vervolgens handmatig vergeleken met een 1:1-vergelijking.

1:1-vergelijking

Bij de 1:1-vergelijking levert de aanvrager tenminste twee vingerafdrukken (spoor 1 en spoor 2) aan waarbij het de bedoeling is om vast te stellen (of uit te sluiten) dat de vingerafdrukken van één en dezelfde persoon zijn.

Een 1:1-vergelijking na 1:n-vergelijking vindt plaats met de geautomatiseerd gematchte vingerafdruk(ken) (spoor 2) en het door aanvrager aangeleverde spoor (spoor 1).

De 1:1-vergelijking is een handmatige vergelijking waarbij twee forensisch onderzoekers (dactyloscopen) van het Centrum voor Biometrie afzonderlijk en onafhankelijk van elkaar de

vingerafdrukken vergelijken zonder dat ze beschikking hebben over zaakinformatie. Vervolgens worden de conclusies van de onderzoekers gecombineerd tot een geconsolideerde conclusie. Bij een ongelijke conclusie of als niet zomaar geïndividualiseerd kan worden gaan de vingerafdrukken naar drie andere onderzoekers. Deze analyseren, vergelijken en concluderen onafhankelijk van elkaar en leggen hun bevinden en conclusie vast. Daarna hebben zij een bijeenkomst waar hun bevindingen met elkaar worden gedeeld en een technische discussie plaatsvindt en een consensus conclusie wordt vastgesteld en gerapporteerd. De geconsolideerde conclusie wordt met de aanvrager van het onderzoek gedeeld in de vorm van een rapport van bevindingen.

Het rapport bevat een van de volgende uitkomsten:

- Het spoor is ongeschikt voor onderzoek
- Het spoor is herkend op getuige
- Het spoor is niet herkend
- Het spoor is niet afkomstig van de potentiële donor
- Individualisatie
- Het spoor is mogelijk afkomstig van de potentiële donor
- Geen overtuigende conclusie mogelijk
- De referentieafdruk heeft onvoldoende kwaliteit[7]

Internationale doorgifte
Nederland, en daarmee de Politie, wisselt vingerafdrukken uit met internationale partners die belast zijn met de opsporing en voorkoming van strafbare feiten. Multilateraal op basis van het Prüm-besluit (opvolger van het Prüm-verdrag) tussen de lidstaten van de Europese Unie.[8] Unilateraal op basis van de Preventing and Combatting of Serious Crime-overeenkomst (hierna: PCSC-overeenkomst) met de Verenigde Staten van Amerika.[9]

Op de GBV-vreemdelingendatabank zijn de EUVIS-verordening en EURODAC-verordening van toepassing. De uitwisseling van gegevens op basis van deze verordening vindt buiten de verwerkingsverantwoordelijkheid van de Politie plaats, daarmee is internationale doorgifte op basis van de EUVIS- en EURODAC-verordening buiten de scope van dit addendum. In uitzondering hierop wordt de doorgifte van vingerprintsets aan EURODAC in het kader van een opsporingsonderzoek wel in scope geplaatst.[10]

Prüm-besluit, PCSC-overeenkomst, en EURODAC.
Prüm-besluit
Het Prüm-besluit is nader uitgewerkt in een uitwerkingsbesluit van de Raad van de Europese Unie.[11]

Op grond van het Prüm-besluit hebben de instanties binnen de lidstaten van de Europese Unie die met de opsporing en vervolging van strafbare feiten belast zijn directe toegang tot elkaars databanken met dactyloscopische gegevens. De lidstaten hebben in deze databanken toegang tot de biometrische

[7] Zie voor de inhoud van de conclusies pagina 6 en 7 van de Vakbijlage Dactyloscopisch onderzoek sporen (Versie 5.0, geldig vanaf september 2022).
[8] Besluit van de Raad van de Europese Unie van 23 juni 2008, 2008/615/JBZ (CELEX:32008D0615)
[9] Overeenkomst tussen de Regering van het Koninkrijk der Nederlanden en de Regering van de Verenigde Staten van Amerika inzake verbetering van de samenwerking bij het voorkomen en bestrijden van ernstige criminaliteit, 's-Gravenhage 19 november 2010 (*Trb.* 2010/321).
's-Gravenhage, 19 november 2010
[10] Art. 20 Verordening (EU) 603/2013 (Eurodac-verordening).
[11] Besluit van de Raad van de Europese Unie van 23 juni 2008, 2008/616/JBZ (CELEX:32008D0616).

gegevens en linkgegevens.[12] De linkgegevens zijn gekoppeld aan individuen, de linkgegevens zijn echter voor de aanvrager niet te herleiden tot een individu. De biometrische gegevens van sporen waarbij een persoon is geïdentificeerd worden zo met deze linkgegevens aan elkaar gekoppeld. Onderzoek in deze database gaat in overeenstemming met de eerder beschreven 1:1-vergelijkingsmethode. Bij een of meerdere matches worden geautomatiseerd de linkgegevens van de gematchte biometrische gegevens aan de aanvragende instantie (de lidstaat) verstrekt. De aanvragende instantie kan dan bij het nationale contactpunt van de eigenaar van de databank via de reguliere weg een internationaal rechtshulpverzoek indienen voor de biografische gegevens onder vermelding van de linkgegevens.

Onderzoek aan de databanken van de lidstaten vindt onder dezelfde voorwaarden plaats die gelden voor het onderzoek aan de nationale vingerafdrukkendatabank(en) van de lidstaten. Als een in Nederland onderzocht strafbaar feit voor een 1:n-vergelijking in aanmerking komt kunnen ook de Prüm-databanken van de lidstaten doorzocht worden. De bevraagde lidstaat beoordeelt dan ook niet de rechtmatigheid van het initiële onderzoek in de HAVANK-strafrechtdatabase door de aanvragende lidstaat.[13]

De Wpg voorziet in de doorgifte met art. 15a welke nader is uitgewerkt in art. 5:5 Bpg.

PCSC-overeenkomst

Met de PCSC-overeenkomst kunnen de opsporingsdiensten van de VS en de opsporingsdiensten van Nederland over en weer in elkaars dactyloscopische gegevens zoeken. De procedure is gelijk aan die van de uitwisseling op grond van het Prüm-besluit (gepseudonimiseerd vergelijken biometrische data waarna een rechtshulpverzoek gedaan wordt na een match).[14] Onderzoek aan de wederzijdse databanken mag uitsluitend plaatsvinden als dit noodzakelijk is in het kader van de opsporing en ter voorkoming van 'ernstige strafbare feiten'.[15] In de PCSC-overeenkomst worden ernstige strafbare feiten aangeduid als gedragingen die met een gevangenisstraf van één jaar of langer bedreigd worden.[16]

Ook creëert het PCSC een mogelijkheid om gegevens (waaronder biometrische gegevens) over een individu proactief, zonder voorafgaande geautomatiseerde vergelijking door de ontvangende partij, te verstrekken. Deze mogelijkheid kan slechts worden benut onder specifieke omstandigheden.[17] Eenvoudig gezegd betreft dit informatie over betrokkenen die gerelateerd worden aan terrorisme. Omdat deze doorgifte geen relatie heeft met het vergelijken van vingerafdrukken valt deze doorgifte buiten de scope van dit addendum.

EURODAC

Op basis van de Eurodac-verordening is er een Europese databank met vingerafdrukken ingesteld die tot doel heeft om vreemdelingen te identificeren en daarmee de verantwoordelijkheid van de lidstaten ten opzichte van een asielaanvraag te bepalen.[18] Deze databank mag ook door de

---

[12] Artikel 8 en artikel 9 van het besluit van de Raad van de Europese Unie van 23 juni 2008, 2008/615/JBZ (CELEX:32008D0615).
[13] Artikel 9 lid 1 van het besluit van de Raad van de Europese Unie van 23 juni 2008, 2008/615/JBZ (CELEX:32008D0615)
[14] Art. 4 en art. 5 van de overeenkomst tussen de Regering van het Koninkrijk der Nederlanden en de Regering van de Verenigde Staten van Amerika inzake verbetering van de samenwerking bij het voorkomen en bestrijden van ernstige criminaliteit, 's-Gravenhage 19 november 2010 (*Trb.* 2010/321).
[15] Art. 3 van de overeenkomst tussen de Regering van het Koninkrijk der Nederlanden en de Regering van de Verenigde Staten van Amerika inzake verbetering van de samenwerking bij het voorkomen en bestrijden van ernstige criminaliteit, 's-Gravenhage 19 november 2010 (*Trb.* 2010/321).
[16] Art. 1 lid 5 van de overeenkomst tussen de Regering van het Koninkrijk der Nederlanden en de Regering van de Verenigde Staten van Amerika inzake verbetering van de samenwerking bij het voorkomen en bestrijden van ernstige criminaliteit, 's-Gravenhage 19 november 2010 (*Trb.* 2010/321).
[17] Art. 11 van de overeenkomst tussen de Regering van het Koninkrijk der Nederlanden en de Regering van de Verenigde Staten van Amerika inzake verbetering van de samenwerking bij het voorkomen en bestrijden van ernstige criminaliteit, 's-Gravenhage 19 november 2010 (*Trb.* 2010/321).
[18] Zie de Dublinverordening, Verordening (EU) 604/2013.

opsporingsautoriteiten van de Europese lidstaten onderzocht worden bij het voorkomen, opsporen of onderzoeken van een 'ernstig strafbaar feit' of 'terroristische misdrijven'.[19] De databank wordt niet door de opsporingsautoriteiten gevuld maar kan in voornoemde gevallen wel onderzocht worden met door de opsporingsautoriteit aan te leveren sporen.

Sporenbeheer buitenlandse sporen
Als de Politie een bevraging doet in de databank van een lidstaat of de VS die een match oplevert volgt een rechtshulpverzoek. De aanvullende gegevens die vervolgens met dit verzoek verkregen zijn worden pas na een 1:1-vergelijking van het originele spoor met de aangeleverde dactyloscopische gegevens opgenomen in de HAVANK-database. Zo wordt geborgd dat er geen verkeerde informatie wordt gekoppeld in de HAVANK-strafrechtdatabase. Ook bevat de aan het dossier gekoppelde dactyloscopische informatie een datum en plaats van de opnamen. Dit betekent dat er eenvoudig onderscheid gemaakt kan worden tussen "eigen" dactyloscopische informatie en door een derde-land verstrekte gegevens.

Politiegegevens

In de GEB Biometrievoorziening is overzichtelijk weergegeven welke categorieën politiegegevens in welk stadium van de verwerking worden verwerkt. De GEB Biometrievoorziening benoemt de omvang van de verwerking van de politiegegevens niet. De omvang van de verwerking is hieronder wel weergegeven.

Omvang	Antwoord
Aantal betrokkenen dat in de verwerking voorkomt, *indien mogelijk per systeem*	Er staan biometrische en biografische gegevens van ongeveer 2 miljoen betrokkenen in de HAVANK-strafrechtdatabase.
Reikwijdte verwerking	Landelijk, niet aan een specifieke regio gebonden.
Duur van de verwerking	De strafrecht-database: Minimaal 20 jaren na een onherroepelijk geworden veroordeling en maximaal 80 jaren na een onherroepelijk geworden veroordeling. In het geval dat een betrokkene niet langer verdachte is of het feit is verjaard worden de gegevens ook uit de strafrecht database verwijderd. Het onderzoeksrapport bij een 1:1 vergelijking wordt voor altijd bewaard bij het Centrum voor Biometrie.
Frequentie van de verwerking	Tussen de 500 en 600 geautomatiseerde 1:n-vergelijkingen van vingerafdrukken per dag en tussen de 6.000 en 10.000 1:1-vergelijkingen per jaar.

[19] Art. 20 en art. 1 lid 1 sub j en k Verordening (EU) 603/2013 (Eurodac-verordening).

Doel van de verwerking

Dactyloscopie heeft als doel om met behulp van vingerafdrukken een persoon te identificeren of uit te sluiten in het kader van het voorkomen, opsporen, vervolgen en berechten van strafbare feiten en het vaststellen van de identiteit van een lijk.

Autorisaties

De leidend Operationeel Specialist van het Centrum voor Biometrie fungeert als bevoegd functionaris voor de politiegegevens die worden verwerkt in het kader van het dactyloscopisch onderzoek. Ook de autorisaties worden door de leidend OS uitgegeven.

Inrichting autorisaties	Ja	Nee	Nadere toelichting
Er is een duidelijke omschrijving van de verwerkingen waartoe een ambtenaar van politie (of persoon) is geautoriseerd	X		Zie IB-analyse. (Bijlage 1)
Er is een autorisatiematrix die een functionaris beheert	X		
Er is een bevoegde functionaris die instemming geeft voor terbeschikkingstelling voor verdere verwerking	X		Verdere verwerking wordt geautoriseerd door de leidend specialist van het Centrum voor Biometrie (Landelijke Eenheid)
De terbeschikkingstelling is geautoriseerd door de aangewezen bevoegd functionaris		X	De functionaris is niet aangewezen middels een aanwijsbesluit.
De daartoe bevoegde functionaris heeft instemming gegeven voor de terbeschikkingstelling	X		De functionaris wordt voor bij elke verstrekking betrokken.
De terbeschikkingstelling is overeenkomstig de autorisatiematrix uitgevoerd	X		Nvt
De terbeschikkingstelling wordt gecontroleerd door een functionaris	X		

Bijzondere politiegegevens

Wettelijke eis (art. 5 Wpg)	Toetsing
De aangegeven te verwerken bijzondere politiegegevens zijn onvermijdelijk voor het doel	De verwerking van biometrische data uit vingerafdrukken is onvermijdelijk voor het te behalen doel. Zonder deze data kan er namelijk geen geautomatiseerde zoekslag plaats vinden in de databases. Zonder de daadwerkelijke vingerafdrukken kunnen de dactyloscopische experts geen één-op-één vergelijking uitvoeren. Deze één-op-één vergelijking is in bepaalde gevallen de enige manier om tot een identificatie van een verdachte te komen.
De te verwerken bijzondere politiegegevens zijn een aanvulling op de andere politiegegevens	De biometrische gegevens zijn steeds gekoppeld aan biografische gegevens van een betrokkene. Slechts op het moment van een één-op-één vergelijking worden de biografische gegevens gepseudonimiseerd om de objectiviteit van de dactyloscoop te waarborgen. De biometrische gegevens worden in aanvulling op andere politiegegevens verwerkt.
De te verwerken bijzondere politiegegevens zijn afdoende beveiligd	De bijzondere politiegegevens worden uitsluitend binnen de rekencentra van de Politie verwerkt. Deze rekencentra zijn afdoende beveiligd. Raadpleging is uitsluitend voorbehouden aan geautoriseerden.

De criteria voor het verwerken van bijzondere politiegegevens ex art. 5 Wpg zijn vervuld.

Noodzakelijkheid, rechtmatigheid en doelbinding

Criteria (art. 3 Wpg)	Verwerking
Proportionaliteit *Staat het belang van de verwerking in verhouding tot de beperking van de persoonlijke levenssfeer?*	De inbreuk die het dactyloscopisch onderzoek vormt op de rechten en vrijheden van betrokkenen staat in verhouding tot het belang van de verwerking. Het maatschappelijk belang bij de opsporing van bij een misdrijf betrokken personen weegt zwaarder dan het belang van de betrokkenen om niet geïdentificeerd te worden. Ditzelfde geldt voor het aanhouden van de database met afbeeldingen en biometrische gegevens van de betrokkenen, deze database wordt namelijk ook gebruikt voor de identificatie van aangehouden verdachten.
Subsidiariteit *Zijn andere minder in de persoonlijke levenssfeer van de burger ingrijpende maatregelen mogelijk?*	Dactyloscopisch onderzoek wordt slechts aangevraagd in die gevallen wanneer er geen uitsluitsel kan worden gegeven over de identiteit van een betrokkene en er geen andere meer eenvoudige methodes meer zijn om de identiteit te achterhalen. De verwerking voldoet daarom aan het subsidiariteitsbeginsel.
Niet bovenmatig *Is de verwerking niet bovenmatig en niet meer dan nodig voor het doel?*	Bij het 1:1-onderzoek worden alleen die gegevens met de dactyloscopische onderzoeker gedeeld die de onderzoeker nodig heeft. Voor het 1:n-onderzoek wordt uitsluitend met geschikte vingerafdrukken in de database(s) gezocht. De gegevensverwerking bij het onderzoek aan de HAVANK-strafrecht database is niet bovenmatig. Hoewel de database 3 miljoen vingerafdruksets bevat zijn de betrokkenen allen gerelateerd aan de strafrechtketen. Gemiddeld genomen recidiveert ongeveer 50% van de meerderjarige veroordeelden.[20] Het is dus te beargumenteren dat er sprake is van een passende verwerking van gegevens in de HAVANK-strafrechtdatabase
Rechtmatigheid van de verkrijging *Zijn de te verwerken gegevens rechtmatig verkregen?*	De database met vinger- en handpalm-afdruksets is gevuld met vingerafdrukken en handpalmafdrukken die voortkomen uit informatie van de BVID-zuil. Deze verkrijging is gebaseerd op art. 55C lid 2 Sv (vingerafdrukken) en art. 61a lid 1 sub b Sv (handpalmen). De vingerafdruksporen die worden aangeleverd in de aanvraag om te worden vergeleken met de database komen uit lopende opsporingsonderzoeken.

[20] Verweij, S. et al., *Recidive onder justitiabelen in Nederland*, Den Haag: WODC, 2021.

Wettelijke verwerkingstermijnen

Wettelijke politietaak Art. 8, 9, 10, 12 of 13 Wpg	Soort gegeven	Wettelijke termijn	Feitelijke termijn	Toetsing
Art. 9	Dactyloscopisch onderzoeksrapport in het kader van een artikel 9 onderzoek met vingerafdrukken en biometrische markers.	Voor zolang de gegevens noodzakelijk zijn voor het opsporingsonderzoek of een half jaar om te bepalen of de politiegegevens aanleiding geven tot een nieuw opsporingsonderzoek. Na deze termijn volgt verwijdering.	Geen verwijdering. Gegevens worden op een netwerkschijf bewaard. Geen vernietiging.	Niet compliant.
Art. 10	Dactyloscopisch onderzoeksrapport met vingerafdrukken en biometrische markers in het kader van een artikel 10 onderzoek.	Voor zolang de politiegegevens noodzakelijk zijn voor het opsporingsonderzoek. Uiterlijk 5 jaren na de laatste mutatie/verwerking die blijk geeft van de noodzaak tot het verwerken van de politiegegevens van betrokkene in het kader van het opsporingsonderzoek.	Geen verwijdering. Gegevens worden op een netwerkschijf bewaard. Geen vernietiging.	Niet compliant
Art. 13	Database met referentiemateriaal: HAVANK-strafrecht	Niet gedefinieerd	Op dit moment wordt voor de HAVANK-strafrechtdatabase het Besluit identiteitsvaststelling verdachten en veroordeelden (BIVV) regime gehanteerd. (art. 9, 9a BIVV) Zie de termijnen in art. 5, 6, 7, 7a BIVV.	De Politie beschouwt voor de HAVANK-strafrechtdatabase het BIVV als art. 13-protocol. De eisen waaraan een art. 13 protocol moet voldoen staan in art. 6:2 Bpg. Het BIVV voldoet niet aan de vereisten van art. 6:2 Bpg. Het BIVV bevat geen beschrijving van de frequentie waarop de verwerkingstermijnen van de gegevens worden gecontroleerd.[21]

[21] Art. 6:2 lid 1 sub d Bpg.

Beoordeling van verstrekkingen aan buitenlandse opsporingsdiensten

Hieronder volgt een toetsing van de doorgifte van politiegegevens aan derde landen op grond van art.15a en 17a Wpg.

Naam derde landen	Toetsing doorgifte
Lidstaten Europese Unie (Prüm)	Art. 15a regelt de ter beschikkingstelling van politiegegevens aan instanties die belast zijn met de politietaak binnen de lidstaten van de Europese Unie. In art. 5:5 Bpg is een bepaling opgenomen die specifiek ziet op de geautomatiseerde doorzending van dactyloscopische gegevens. Art. 15a lid 1 Wpg vereist voor de ter beschikkingstelling van politiegegevens dat er een rechtsinstrument op grond van het VwEU aan ten grondslag ligt. Het Prüm-besluit beantwoordt aan deze eis. Terbeschikkingstelling van politiegegevens vindt plaats conform de in art. 15a Wpg en art. 5:5 Bpg beschreven procedures. De terbeschikkingstelling van de HAVANK-strafrechtdatabase ten behoeve van geautomatiseerde doorzoeking voldoet aan de criteria van art. 15a Wpg. De afhandeling van het rechtshulpverzoek volgende op de geautomatiseerde vergelijking is niet in scope van onderhavig addendum.
Lidstaten Europese Unie (Eurodac)	Omdat de Eurodac-database niet aangehouden wordt door een instantie die belast is met de opsporing en voorkoming van strafbare feiten is art. 15a Wpg niet van toepassing. Dan blijft art. 17a Wpg over. Doorgifte van sporen via Eurodac betreft een zeer beperkte verwerkingsactiviteit, uitsluitend het spoor wordt aangeleverd welke na een maand weer verwijderd wordt.[22] Het orgaan dat Eurodac beheert is een orgaan van de Europese Unie, de Eurodac-databank voldoet aan de vereisten van gegevensbescherming van de Europese Unie. Verstrekking van vingerafdruksporen in het kader van een opsporingsonderzoek voldoet daarom aan de vereiste van doorgifte ex art. 17a lid 1 Wpg.
Verenigde Staten van Amerika	Er is een adequaatheidsbesluit van de Europese Commissie dat vaststelt dat de VS voldoet aan Europese standaarden voor gegevensverwerking.[23] Dit betekent dat doorzending van politiegegevens op basis van art. 17a lid 1 Wpg plaats kan vinden mits er voldaan wordt aan de volgende vereisten: **Vereisten doorgifte** 1. Doorgifte is noodzakelijk in het kader van de uitvoering van de politietaak zoals bedoeld in art. 3 Politiewet 2012. 2. In het geval de politiegegevens verkregen zijn van een derde land of lidstaat moet, behoudens internationale overeenkomsten en verdragen, voor verdere doorgifte toestemming worden verkregen van het betreffende land of de lidstaat. (art. 17a lid 4 Wpg) 3. De doorgifte voldoet aan art. 5:1 Bpg: 3.1. De politiegegevens worden door de VS uitsluitend voor het doel gebruikt waarvoor ze zijn verstrekt: het opsporen en voorkomen van strafbare feiten waar een gevangenisstraf van ten minste één jaar op staat. In het geval dat er afgeweken wordt van het oorspronkelijke doel van de verwerking is dit uitsluitend ten dienste van de voorkoming van een onmiddellijke en ernstige bedreiging van de openbare veiligheid. 3.2. Verdere verwerking door de VS voor een ander doel kan alleen na toestemming van de

[22] Art. 20 en art. 33 lid 5 Eurodac-verordening.
[23] Besluit 2023/1795/EU van de Commissie van 10 juli 2023 overeenkomstig Verordening (EU) 2016/679 van het Europees Parlement en de Raad inzake het passende niveau van bescherming van persoonsgegevens krachtens het EU-VS-kader voor gegevensbescherming (*PbEU* 2023, L 231/118).

Naam derde landen	Toetsing doorgifte
	Politie. 3.3. Doorgifte van bijzondere politiegegevens (zoals de dactyloscopische biometrische gegevens) vindt alleen plaats als dit onvermijdelijk is voor de beantwoording van de door de Amerikaanse politieautoriteit gestelde vraag. 3.4. Gegevens dienen door de VS te worden verwijderd zodra de doeleinden waaronder de gegevens verkregen zijn verwezenlijkt zijn, behoudens noodzakelijke verdere verwerking. 3.5. Er is een methode om fouten te corrigeren in gegevens als die op een later moment door de Politie geconstateerd worden. **Beoordeling** 1. Omdat de dactyloscopische gegevens uitsluitend worden vergeleken in het kader van de opsporing van gedragingen die worden bedreigd met gevangenisstraf van ten minste één jaar vindt de doorgifte plaats in het kader van de daadwerkelijke strafrechtelijke handhaving van de rechtsorde. Daarmee is aan criterium 1 voldaan. 2. De aan Nederland geleverde gegevens bevatten steeds de plaats en tijd van de opname van het dactyloscopische spoor. In het geval er een verzoek gedaan wordt over sporen waarvan de oorsprong in een ander land ligt wordt doorverwezen naar dit land. Zo wordt voldaan aan het vereiste van toestemming. Deze eis is ook opgenomen in art. 13 lid 2 van de PCSC-overeenkomst.[24] 3. Beoordeling naar art. 5:1 Bpg: 3.1. Het PCSC legt deze verplichting op aan beide verdragspartijen. 3.2. Dit is geregeld in het PCSC met de verwijzing naar het Verdrag inzake wederzijdse rechtshulp tussen Nederland en de VS.[25] 3.3. Art. 12 lid 2 sub a PCSC geeft als voorwaarde voor de verwerking dat de informatie 'ter zake dienend' moet zijn. Daarmee wordt voldaan aan de derde voorwaarde uit art. 5:1 Bpg. 3.4. Op grond van art. 13 lid 4 PCSC worden de gegevens die ten behoeve van geautomatiseerde vergelijking zijn verstrekt na de vergelijking door de bevraagde partij verwijderd. Art. 12 lid 2 sub b PCSC regelt de algemene voorwaarden voor de bewaartermijn van de andere verstrekte en ontvangen politiegegevens. Deze voorwaarden voldoen aan art. 5:1 Bpg. 3.5. Het PCSC creëert een mogelijkheid om fouten te herstellen. De Politie heeft echter de staande beleidsopvatting dat er geen verkeerde registraties bestaan omdat deze altijd worden opgemaakt onder de dan bekende omstandigheden. Verstrekking op basis van het PCSC voldoet aan de vereisten van de Wpg en het Bpg.

[24] Overeenkomst tussen de Regering van het Koninkrijk der Nederlanden en de Regering van de Verenigde Staten van Amerika inzake verbetering van de samenwerking bij het voorkomen en bestrijden van ernstige criminaliteit, 's-Gravenhage 19 november 2010 (*Trb.* 2010/321).

[25] Artikel 13 lid 1 van de overeenkomst tussen de Regering van het Koninkrijk der Nederlanden en de Regering van de Verenigde Staten van Amerika inzake verbetering van de samenwerking bij het voorkomen en bestrijden van ernstige criminaliteit, 's-Gravenhage 19 november 2010 (*Trb.* 2010/321); Artikel 11bis van het Verdrag tussen het Koninkrijk der Nederlanden en de Verenigde Staten van Amerika aangaande wederzijdse rechtshulp in strafzaken, 's-Gravenhage 12 juni 1981 (*Trb.* 1981, 188).

POLITIE

Memo

Risico's

Thema	Risico categorieën	Risico omschrijving voor betrokkene en/of organisatie	Kans	Impact	Risico Inschatting	Maatregelen	Restkans	Restimpact	Restrisico inschatting
1. Organisatie	1.2. Rechtmatigheid	De verwerking voor ondersteuning van de politietaak (art. 13 Wpg) heeft geen schriftelijke vastlegging (protocol ex art. 13 lid 1 Wpg) waarin o.a. de frequentie van de controle op de verwerkingstermijnen is vastgelegd.	5	1	5	Beschrijf in een addendum de frequentie waarop de verwerkingstermijnen van de gegevens in de HAVANK-strafrechtdatabase gecontroleerd worden en stel dit vast als onderdeel van het art. 13 protocol.	0	0	0
1. Organisatie	1.2. Rechtmatigheid	De sporen in de HAVANK-strafrechtdatabase worden niet tijdig verwijderd vanwege het ontbreken van de afloopberichten vanuit de strafrechtketen. De betrokkene loopt zo het risico, dat er te veel gegevens worden verwerkt. Ook dreigt hier voor de organisatie een boete en imagoschade.	5	1	5	Treed in overleg met de strafrechtketen om consistent en wellicht geautomatiseerd afloopberichten te verkrijgen.	0	0	0
1. Organisatie	1.7. Autorisatie	De geautoriseerde bevoegd functionaris (leidend specialist van het Centrum voor Biometrie) is niet als zodanig	5	2	10	Wijs de bevoegd functionaris aan met een besluit.	0	0	0

		aangewezen middels een besluit.							
1. Organisatie	**1.8. Verwerkings-termijnen**	De verwerkingstermijnen worden niet nageleefd ten aanzien van de dactyloscopische onderzoeksrapporten waardoor de verwerking langer plaatsvindt en de politiegegevens langer toegankelijk zijn dan is toegestaan.	5	3	15	Pas systemen en procedures aan om de verwerkingstermijnen na te leven. Geef de medewerkers de nodige instructies zodat de rapporten tijdig verwijderd worden.	1	1	1

POLITIE

Memo

Bijlagen

Bijlage 1 IB analyse CATCH/HAVANK.

Gegevensbeschermings effectbeoordeling (GEB) Wpg

Uitvoeren digitaal onderzoek

5.1.2.e

Definitief

Versie 1.0

Versie datum 22 februari 2024

Versiegeschiedenis

Versie	Versie datum	Samenvatting van de aanpassing	Gemarkeerde wijzigingen
0.1	30-11-2023	Eerste opzet GEB Uitvoeren digitaal onderzoek	
0.2	04-12-2023	Tweede opzet GEB Uitvoeren digitaal onderzoek	
0.3	19-02-2023	Derde opzet GEB Uitvoeren digitaal onderzoek	
1.0	22-02-2024	Definitieve versie GEB Uitvoeren digitaal onderzoek	

Distributie

Versie	Verzend datum	Naam	Functie
0.1	30-11-2023	5.1.2.e	Privacy adviseur
0.2	04-12-2023	5.1.2.e en 5.1.2.e	Materiedeskundigen
0.3	04-12-2023	5.1.2.e en 5.1.2.e	Privacyfunctionaris
1.0	10-04-2024	Wilbert Paulissen en 5.1.2.e	Portefeuillehouder Strategisch adviseur

Review commentaar

Versie	Wanneer	Wie	Functie
0.1	01-12-2023	5.1.2.e	Privacy adviseur
0.2	12-12-2023	5.1.2.e en 5.1.2.e	Materiedeskundigen
0.3	16-01-2024	5.1.2.e en 5.1.2.e	Privacyfunctionaris

Inhoudsopgave

Basisinformatie

Datum	Donderdag 22 februari 2024
Naam van de verwerking zoals aangemeld in 5.1.2.i	Uitvoeren digitaal onderzoek
Ingangsdatum van de verwerking	Bestaande verwerking
Gemandateerd verwerkingsverantwoordelijk Portefeuillehouder en eenheid	Wilbert Paulissen
Politieonderdeel waar de verwerking plaatsvindt	Specialistische opsporing
Contactpersoon m.b.t. deze verwerking	5.1.2.e - strategisch adviseur
Privacyfunctionaris portefeuille	• 5.1.2.e • 5.1.2.e

Betrokken bij deze GEB	**Naam**
Vanuit het Programma Intensivering Privacy	• 5.1.2.e Privacy adviseur, Programma Intensivering Privacy 5.1.2.e • 5.1.2.e Privacy adviseur en 5.1.2.e, Programma Intensivering Privacy (Interne reviewer van deze GEB) • 5.1.2.e Informatiebeveiliger, Programma Intensivering Privacy (Uitvoerder IB-analyse)
Materiedeskundigen	• 5.1.2.e Digitaal rechercheur, 5.1.2.e • 5.1.2.e Digitaal rechercheur, 5.1.2.e • 5.1.2.e Tactisch rechercheur, 5.1.2.e • 5.1.2.e Operationeel Specialist TO/ Digitale expertise, 5.1.2.e

Functionaris gegevensbescherming	5.1.2.e
Advies FG nodig:	Nee
Datum	Donderdag 22 februari 2024
Toelichting: Op basis van het beleidskader registerplicht en GEB is de adviserende rol van de FG rondom de uitvoering van de GEB's gemandateerd aan de privacyfunctionaris. Op basis van het hoofdproces registerplicht en GEB is de privacyfunctionaris reviewer (degene die de GEB controleert en advies geeft op de uitgevoerde GEB).	

Gezien door verwerkingsverantwoordelijke

Naam	
Functie	
Datum	
Opmerkingen	

1. Managementsamenvatting

1.1. Hoog risico verwerking

Deze managementsamenvatting van de gegevensbeschermingseffectbeoordeling (hierna: GEB) is bedoeld voor besluitvorming door de verwerkingsverantwoordelijke. Het bevat de belangrijkste bevindingen, risico´s en maatregelen voor de onderzochte verwerking.
Op de verwerking van de portefeuille zijn een GEB en een informatiebeveiligingsanalyse uitgevoerd op grond van de Wet politiegegevens (hierna: Wpg). Een GEB voer je uit als een gegevensverwerking waarschijnlijk een hoog privacy-risico oplevert voor de personen over wie de politie gegevens verwerkt.

De criteria voor een hoog risico verwerking zijn bepaald door de Europese toezichthouder en het beleid van de politie. Deze criteria zijn opgenomen in de 'QuickScan' die wordt uitgevoerd in het systeem 5.1.2.i. Hier vindt ook de registratie van de verwerking plaats. De criteria voor de hoog risico verwerkingen zijn opgenomen in de toelichting bij het GEB formulier.

De verwerking is als een hoog risico verwerking aangemerkt omdat:

- bij het uitvoeren van digitaal onderzoek politiegegevens van zeer persoonlijke aard kunnen worden verwerkt, zoals bijzondere politiegegevens;
- er op grote schaal politiegegevens worden verwerkt;
- het uitvoeren van digitaal onderzoek grote impact op de betrokkenen kan hebben die als kwetsbare personen dienen te worden beschouwd.

1.2. Aanpak

Deze GEB is tot stand gekomen in overleg met de adviseurs van de portefeuille en materiedeskundigen.

Betrokken bij de uitvoering van deze GEB en de gevolgde aanpak:

Betrokken bij de GEB

- 5.1.2.e, privacy adviseur 5.1.2.e
- 5.1.2.e, privacy adviseur, 5.1.2.e en interne reviewer van deze GEB
- 5.1.2.e, informatiebeveiliger, uitvoerder informatiebeveiligingsanalyse
- 5.1.2.e, Digitaal rechercheur, 5.1.2.e
- 5.1.2.e, Digitaal rechercheur, 5.1.2.e
- 5.1.2.e, Tactisch rechercheur, 5.1.2.e
- 5.1.2.e, Operationeel Specialist TO/ Digitale expertise, 5.1.2.e

Gevolgde aanpak

5.1.2.e, Senior Tactische Opsporing 5.1.2.e, heeft de penvoerder van deze GEB in contact gebracht met verschillende materiedeskundigen. In persoonlijke gesprekken met de materiedeskundigen is de verwerking 'Uitvoeren digitaal onderzoek' ten behoeve van de GEB in kaart gebracht. Op basis van de verkregen informatie is een beeld geschetst van de feitelijke werkwijze met betrekking tot het uitvoeren van digitaal onderzoek, die vervolgens als input voor de GEB is gebruikt. Naast de gevoerde gesprekken met de materiedeskundigen is op Agora informatie en documenten over het proces geraadpleegd en is relevante wet- en regelgeving bestudeerd voor de juridische toetsing.

1.3. Belangrijkste bevindingen verwerking

Korte beschrijving van de belangrijkste aangetroffen privacy en IB-issues en risico's:

- Een onderzoeksdossier wordt door de opsporingsambtenaar van politie in de praktijk pas op afgehandeld gezet na een afdoeningsbericht van het OM. Doordat dit proces niet is geautomatiseerd en/of een afdoeningsbericht structureel achterwege blijft, komt het in de praktijk veelvuldig voor dat dossiers met daarin politiegegevens blijven staan op status "verwerken" en daardoor gegevens langer worden verwerkt dan wettelijk is toegestaan. Dit maakt tevens dat er langer dan noodzakelijk is inbreuk wordt gemaakt op de privacy van betrokkenen. Hierdoor kan er imagoschade optreden of kan de politie een last onder

bestuursdwang of bestuurlijke boete opgelegd krijgen van de AP en andere onderzoeken die starten met deze gegevens kunnen een onrechtmatig basis hebben.

- Momenteel worden politiegegevens die in het politiesysteem BVH staan niet structureel vernietigd. Hierdoor worden politiegegevens langer verwerkt dan de wettelijke termijnen en is er sprake van een onrechtmatige gegevensverwerking. Als gevolg hiervan kan imagoschade optreden of kan de politie een last onder bestuursdwang of bestuurlijke boete opgelegd krijgen van de AP. Wel wordt de toegankelijk tot deze gegevens na 5 jaar beperkt en zijn enkel aangewezen poortwachters geautoriseerd in het kader van hernieuwd verwerken.
- Politiegegevens die in Summ-IT worden opgeslagen worden niet vernietigd. Daarnaast is er geen bewaartermijn met beperkte toegankelijkheid ingericht en zijn er geen poortwachters aangesteld. Hierdoor zijn politiegegevens onvoldoende beschermd, worden ze langer verwerkt dan de wettelijke termijnen en is er sprake van een onrechtmatige gegevensverwerking. Als gevolg hiervan kan imagoschade optreden of kan de politie een last onder bestuursdwang of bestuurlijke boete opgelegd krijgen van de AP en andere onderzoeken die starten met deze gegevens kunnen een onrechtmatig basis hebben.
- Afgesloten Verwerkersovereenkomsten worden structureel niet in het daarvoor bestemde register (5.1.2.I) opgeslagen. Hierdoor kunnen verwerkersovereenkomsten niet meer teruggevonden worden en is het onduidelijk of de naleving van de wet door de verwerker is afgedwongen met een juridisch dwingend instrument. Er kan hierdoor geen controle vinden op de naleving van de gemaakte afspraken.
- Het is onduidelijk of er verwerkersovereenkomsten zijn gesloten met partners als 5.1.2.I en 5.1.2.I . De verwerkersovereenkomsten zijn niet in het verwerkingsregister 5.1.2.I geüpload en het is niet duidelijk waar ze wel zijn opgeslagen. Het risico bestaat dat partners minder waarborgen treffen dan noodzakelijk is om de privacy van de betrokkenen te beschermen. Als gevolg hiervan kunnen er datalekken optreden, worden gegevens mogelijk langer bewaard dan is toegestaan, worden gegevens mogelijk voor eigen doeleinden gebruikte etc. Zonder verwerkers-overeenkomst kan er geen controle plaatsvinden op naleving van de afspraken.

1.4. Maatregelen

De GEB en de IB-analyse leiden tot risico's en maatregelen gericht op onder meer de werkprocessen, de medewerkers en de systemen. Meer gedetailleerde informatie over de uitgevoerde risico analyses is te vinden in onderdelen C en D van deze GEB. De analyses voor informatiebeveiliging zijn beschikbaar in het IB-kwartier.

De belangrijkste risico´s en maatregelen zijn:

- Inventariseer in hoeverre wordt voldaan aan de wettelijke bewaar- en vernietigingstermijnen en pak de geconstateerde afwijkingen op.
- Maak afspraken met het OM over tijdige (bij voorkeur geautomatiseerde) kennisgeving met betrekking tot het sluiten van een dossier, zodat de wettelijke bewaar- en vernietigingstermijnen gaan lopen.
- Richt een procedure in over hoe er in de praktijk moet worden omgegaan met politiegegevens die voor cold case onderzoek langer worden bewaard dan de termijn die op grond van de Wpg is bepaald. Bepaal welke gegevens langer dan tien jaar bewaard kunnen worden en vernietig de overige gegevens waarvoor de bewaartermijn is verstreken.
- Vernietig politiegegevens die in Summ-IT staan waarvan de bewaartermijn is verstreken.
- Richt een (geautomatiseerd) proces in met betrekking tot toezicht en controle op de bewaar- en vernietigingstermijnen van politiegegevens.
- Beoordeel per verwerking welke ketenpartners bij de verwerking betrokken zijn. Toets vervolgens of de ketenpartner een verwerker is. Zo ja, kijk of er een verwerkersovereenkomst is afgesloten. Sluit een verwerkersovereenkomst af indien dit niet is gebeurd. Sla de ondertekende verwerkersovereenkomst op onder de juiste verwerking in 5.1.2.I
- Controleer of een verwerkersovereenkomst is afgesloten. Sluit een verwerkersovereenkomst af indien deze ontbreekt. Is er wel een verwerkersovereenkomst, controleer of deze actueel is. Sla de verwerkersovereenkomst op in 5.1.2.I

1.5. Vervolgproces

Het vervolgproces voor de portefeuillehouder ten aanzien van de maatregelen:

De GEB beschrijft de maatregelen die nodig zijn om de privacyrisico's voor de betrokkenen te mitigeren die volgen uit de bevindingen ten aanzien van de verwerking 'Uitvoeren digitaal onderzoek'. De portefeuille Specialistische Opsporing heeft de taak deze mitigerende maatregelen te implementeren. Daarom dient na de ondertekening en overhandiging van de GEB een besluitvormingstraject over de implementatie van de mitigerende maatregelen te volgen. De portefeuillehouder is verantwoordelijk voor het (laten) opstellen van een plan van aanpak om de implementatie van de maatregelen te realiseren. Gedurende de risicomitigatie is de Primus Inter Pares (PIP) die door de portefeuillehouder is aangewezen verantwoordelijk voor de verwerking 'Uitvoeren digitaal onderzoek'. Met betrekking tot individuele applicaties kan bij het Programma Intensivering Privacy nadere informatie worden opgevraagd, zoals informatie over uitgevoerde IB–analyses.

A. Beschrijving kenmerken gegevensverwerking

In deel A beschrijf je de onderdelen van de (voorgenomen) gegevensverwerking. Het gaat om de feitelijke situatie. Essentieel is dat de feiten helder en volledig zijn, want in deel B van de GEB vindt de beoordeling plaats.

1. Beschrijving verwerking

1a. Geef een korte beschrijving van de context van de verwerking
Beschrijf waar in de organisatie de verwerking plaatsvindt en de beleidsdoelstellingen van de verwerking.

Antwoord:

Algemeen
De politie is waakzaam en dienstbaar aan de waarde van de rechtstaat. Dit doet de politie door afhankelijk van de situatie gevraagd en ongevraagd te beschermen, te begrenzen en te bekrachtigen. De politietaak omvat het zorgen voor de daadwerkelijke handhaving van de rechtsorde en het verlenen van hulp aan hen die deze behoeven.[1] Daadwerkelijke handhaving valt uiteen in 'openbare orde handhaving' en 'strafrechtelijke handhaving'. Het opsporen van strafbare feiten behoort tot de kerntaak van de politie en valt onder de strafrechtelijke handhaving van de rechtsorde. In dat geval treedt de ambtenaar van politie op onder het gezag van de Officier van Justitie, vertegenwoordiger van het Openbaar Ministerie (OM).[2] In de praktijk is de opsporingsambtenaar[3] van politie belast met de opsporing van strafbare feiten.[4] De opsporingsambtenaar van politie heeft op grond van de wet, waaronder het Wetboek van Strafvordering (Sv) een aantal (bijzondere) opsporingsbevoegdheden die hij ten behoeve van het opsporingsonderzoek mag inzetten. De (bijzondere) opsporingsbevoegdheden zijn ingrijpend en vormen een groot inbreuk op de persoonlijke levenssfeer van de verdachte(n)[5] en eventuele overige betrokkenen. Om deze reden mogen de (bijzondere) opsporingsbevoegdheden alleen onder specifiek in de wet benoemde voorwaarden worden ingezet.

Context verwerking
De context van de verwerking is het uitvoeren van digitaal onderzoek door de digitaal rechercheur van politie. Digitaal onderzoek wordt uitgevoerd met als doel om informatie te verkrijgen die verder richting kan geven aan het opsporingsonderzoek of in de rechtszaak als bewijslast tegen de verdachte(n) gebruikt kan worden. Digitaal onderzoek betreft het veiligstellen en analyseren van informatie die uit de inbeslaggenomen elektronische gegevensdragers en/of geautomatiseerde werken worden verkregen. Elektronische gegevensdrager zijn voorwerpen die bedoeld zijn om gegevens op te slaan, maar waarvoor andere apparatuur nodig is om die gegevens te kunnen waarnemen. Denk hierbij aan: een usb-stick, een SD-kaart, een externe harde schijf etc. Geautomatiseerd werk zijn apparatuur die 'zelfstandig' gegevens kunnen opslaan, verwerken en overdragen. Denk hierbij aan: een computer, een laptop, een smartphone, een horloge, een auto, een camera, een navigatiesysteem etc. Digitaal onderzoek is een opsporingsbevoegdheid die de opsporingsambtenaar van politie ten behoeve van een opsporingsonderzoek kan uitvoeren.

Inrichting verwerking
Iedere politie-eenheid heeft een team digitale opsporing. Dit team is onder andere belast met het verzamelen van digitale sporen door inbeslaggenomen elektronische gegevensdragers en/of geautomatiseerde werken veilig te stellen. Het veiligstellen van inbeslaggenomen elektronische gegevensdragers en/of geautomatiseerde werken gebeurt door de digitaal rechercheur. De tactisch rechercheur analyseert de verkregen informatie en geeft hier betekenis aan. De verwerking 'Uitvoeren digitaal onderzoek' behoort tot de portefeuille Specialistische Opsporing.

[1] Art. 3 Politiewet 2012
[2] Art. 12 lid 1 Politiewet 2012
[3] Art. 141 sub b en c Wetboek van Strafvordering
[4] Art. 127 Wetboek van Strafvordering
[5] Art. 27 Wetboek van Strafvordering

Beschrijf op hoofdlijnen de verwerking
Beschrijf waar de verwerking betrekking op heeft, waar de verwerking begint en eindigt zodat de scope van de verwerkingsverantwoordelijkheid duidelijk wordt.

Antwoord:

Scope van de GEB
De scope van deze GEB is de verwerking van politiegegevens door de opsporingsambtenaar van politie bij het uitvoeren van digitaal onderzoek. Onder digitaal onderzoek wordt verstaan het veiligstellen en analyseren van informatie die uit de inbeslaggenomen elektronische gegevensdragers en/of geautomatiseerde werken worden verkregen. Buiten de scope van deze GEB valt het verwerken van online informatie door de internetrechercheur.

1c. Samenvatting uitvoeren digitaal onderzoek
Om een goed beeld te krijgen in welke context politiegegevens worden verwerkt bij het uitvoeren van digitaal onderzoek, is het van belang helder zicht te krijgen in de stappen die worden doorlopen. Hiervan vindt u onderstaand een beschrijving.

Antwoord:

Uitvoeren digitaal onderzoek – welke stappen worden doorlopen?

1. Melding
De politie krijgt via verschillende kanalen meldingen van vermoedelijke wetsovertredingen. Iedere betrokkenheid van de opsporingsambtenaar van politie is om na te gaan of er daadwerkelijk sprake is van een wettelijke overtreding, welke reden is voor het starten van een strafrechtelijk onderzoek zoals bedoeld in het wetboek van Strafvordering. Een melding van een vermoedelijke wetsovertreding kan bij de politie via verschillende kanalen binnenkomen. Bijvoorbeeld via het Regionaal Service Centrum (RSC), het Operationeel Centrum (OC), door een melding op het basisteam, een anonieme melding, uit een lopend opsporingsonderzoek of door een melding van het Team Criminele Inlichtingen (TCI). Een melding kan bijvoorbeeld zijn dat een bepaald persoon vermoedelijk in het bezit is van kinderporno. Als een melding bij het RSC of OC binnenkomt wordt deze door de centralist in de Servicemodule ingevoerd en doorgestuurd naar het basisteam of het opsporingsteam van de regio waarbinnen de verblijfsplaats van de verdachte valt. De Servicemodule heeft een koppeling met het politiesysteem BVH waardoor de melding automatisch naar BVH wordt overgezet. Op het basisteam wordt de melding in BVH opgepakt. Betreft het een anonieme melding of een melding van het TCI, dan komt deze rechtstreeks bij het opsporingsteam van politie binnen via een speciale ‘artikel 12 Wpg’ mailbox. Volgt de melding uit een lopend opsporingsonderzoek, dan geeft de betreffende afdeling van de politie de melding per mail of telefonisch door aan het opsporingsteam van politie van de regio waarbinnen de verblijfsplaats van de verdachte valt.

2. Start strafrechtelijk onderzoek
Als een melding op het basisteam van politie is binnengekomen, bepaalt de Officier van Dienst Politie (OvD-P) welke diensten hij noodzakelijk acht voor de handhaving van de openbare orde en zo nodig voor de eerste stappen van een strafrechtelijk onderzoek in afwachting van de Officier van Dienst Recherche (OvD-R). De OvD-R leidt het onderzoek ter plaatse en stuurt rechercheurs en specialistische diensten aan. Bijvoorbeeld Team Digitale Opsporing (TDO) en de digitaal rechercheur. De digitaal rechercheur bekijkt ter plaatse welke elektronische gegevensdragers en/of geautomatiseerde werken voor digitaal onderzoek inbeslaggenomen moeten worden. In sommige gevallen worden elektronische gegevensdragers en/of geautomatiseerde werken ter plaatse door de digitaal rechercheur veiliggesteld om dataverlies te voorkomen. Na het doorzoeken geeft de digitaal rechercheur van politie aan de opsporingsambtenaar van politie van het onderzoeksteam door welke elektronische gegevensdragers en/of geautomatiseerde werken ter plaatse zijn aangetroffen en voor digitaal onderzoek inbeslaggenomen moeten worden. De opsporingsambtenaar van politie van het onderzoeksteam is formeel degene die de elektronische gegevensdragers en/of geautomatiseerde werken in beslag neemt en administratief afhandelt. Is de doorzoeking ter inbeslagname ineen openbare ruimte, dan is er geen redelijke verwachting van privacy en zijn opsporingshandelingen vrijwel altijd proportioneel. Hierdoor mag de opsporingsambtenaar van politie van het onderzoeksteam zonder schriftelijke machtiging van de (Hulp)Officier van Justitie (H)OvJ) de openbare ruimte doorzoeken. Is de doorzoeking in een gesloten ruimte, niet zijnde een woonruimte, dan mag de opsporingsambtenaar van politie van het onderzoeksteam deze alleen doorzoeken met een schriftelijke machtiging

van de HOvJ. Betreft de gesloten ruimte een woonruimte, dan is een machtiging van de Rechter-Commissaris (RC) nodig.

3. Schriftelijke machtiging
Als de opsporingsambtenaar van politie een gesloten ruimte, niet zijnde een woonruimte, wil doorzoeken ter inbeslagname heeft de opsporingsambtenaar van politie een schriftelijke machtiging tot binnentreding van de HOvJ nodig. In de praktijk vraagt de opsporingsambtenaar van politie mondeling een machtiging tot binnentreden aan bij de HOvJ. De HOvJ toetst aan de hand van de wet of binnentreden in het specifieke geval is toegestaan. De HOvJ maakt vervolgens in BVH of Summ-IT een machtiging tot binnentreding en voegt deze aan het onderzoeksdossier. Is de doorzoeking ter inbeslagname in een woonruimte, dan heeft de opsporingsambtenaar van politie voor de doorzoeking ter inbeslagname een schriftelijke machtiging van de RC nodig. De opsporingsambtenaar van politie vraagt een schriftelijke machtiging bij de RC aan door in Summ-IT het 'aanvraag proces-verbaal binnentreden' in te vullen en naar de RC te sturen.

4. Briefing
Als de opsporingsambtenaar van politie ter plaatse gaat voor een doorzoeking, volgt eerst een briefing of kort overleg met de overige betrokken opsporingsambtenaren van politie. Als de digitaal rechercheur mee gaat naar de doorzoeking is ook de digitaal rechercheur bij de briefing of kort overleg aanwezig. Tijdens de briefing of kort overleg wordt besproken wat het vermoedelijk gepleegde strafbare feit is op basis waarvan de doorzoeking ter inbeslagname wordt uitgevoerd, welke elektronische gegevensdragers en/of geautomatiseerde werken er vermoedelijk bij de doorzoeking aangetroffen zullen worden en voor digitaal onderzoek inbeslaggenomen worden. Als de digitaal rechercheur niet meegaat naar de doorzoeking geeft hij aan de opsporingsambtenaar van politie door welke elektronische gegevensdragers en/of geautomatiseerde werken mogelijk waardevol kunnen zijn voor digitaal onderzoek en inbeslaggenomen moeten worden.

5. Doorzoeking ter inbeslagname openbare ruimte
Als de doorzoeking in een openbare ruimte gebeurt en het gepleegde strafbare feit een misdrijf betreft als genoemd in artikel 67 lid 1 Sv, mag de opsporingsambtenaar van politie zonder schriftelijke machtiging de plaats doorzoeken. De digitaal rechercheur bekijkt welke elektronische gegevensdragers en/of geautomatiseerde werken inbeslaggenomen moeten worden voor digitaal onderzoek. Als de digitaal rechercheur niet aanwezig is bij de doorzoeking doet de opsporingsambtenaar van politie dit. Het doorzoeken ter inbeslagname in een openbare ruimte gebeurt onder leiding van de OvD-P. Na de doorzoeking geeft de digitaal rechercheur aan de opsporingsambtenaar van politie door welke elektronische gegevensdragers en/of geautomatiseerde werken ter plaatse zijn aangetroffen en voor digitaal onderzoek inbeslaggenomen moeten worden. De opsporingsambtenaar van politie legt alle elektronische gegevensdragers en/of geautomatiseerde werken die de digitaal rechercheur voor digitaal onderzoek in beslag wil nemen fysiek voor aan de OvD-P of de ter plaatse gekomen OvD-R. De OvD-P of OvD-R bepaalt welke elektronische gegevensdragers en/of geautomatiseerde werken in beslag genomen mogen worden voor digitaal onderzoek. Als de OvD-P dit heeft bepaald, moeten de inbeslaggenomen elektronische gegevensdragers en/of geautomatiseerde werken zo spoedig mogelijk ter beoordeling worden voorgelegd aan de HOvJ. Heeft de OvD-R bepaald welke elektronische gegevensdragers en/of geautomatiseerde werken in beslag worden genomen, dan hoeft dit niet omdat de OvD-R ook HOvJ is. De opsporingsambtenaar van politie neemt de inbeslaggenomen elektronische gegevensdragers en/of geautomatiseerde werken mee naar het politiebureau.

6. Doorzoeking ter inbeslagname gesloten ruimte
Voor de opsporingsambtenaar van politie de plaats, zijnde een woonruimte, doorzoekt ter inbeslagname zal hij zich legitimeren en mededeling doen van het doel van de doorzoeking. Voor zover dit mogelijk is zal de opsporingsambtenaar van politie de schriftelijke machtiging tot binnentreding tonen. In de praktijk is bij een doorzoeking ter inbeslagname de RC aanwezig. De RC is de autoriteit die de doorzoeking ter inbeslagname op grond van artikel 110 Sv opent en samen met de OvJ, gemandateerd naar de HOvJ leidt. Als de doorzoeking is geopend bekijkt de digitaal rechercheur welke elektronische gegevensdragers en/of geautomatiseerde werken in de woonruimte aanwezig zijn en voor digitaal onderzoek inbeslaggenomen moeten worden. Als de digitaal rechercheur niet aanwezig is bij de doorzoeking doet de opsporingsambtenaar van politie dit. Na de doorzoeking geeft de digitaal rechercheur aan de opsporingsambtenaar van politie door welke elektronische gegevensdragers en/of geautomatiseerde werken ter plaatse zijn aangetroffen en voor digitaal onderzoek inbeslaggenomen moeten worden. De opsporingsambtenaar van politie legt alle elektronische gegevensdragers en/of geautomatiseerde werken die de digitaal rechercheur voor digitaal onderzoek in beslag wil nemen fysiek voor aan de RC. De RC bepaalt welke elektronische gegevensdragers en/of geautomatiseerde werken in beslag genomen mogen worden voor digitaal

onderzoek. De opsporingsambtenaar van politie neemt de inbeslaggenomen elektronische gegevensdragers en/of geautomatiseerde werken mee naar het politiebureau.

7. Kennisgeving van inbeslagneming

Op het politiebureau maakt de opsporingsambtenaar van politie in Summ-IT een proces-verbaal van doorzoeking op. In het proces-verbaal van doorzoeking geeft de opsporingsambtenaar van politie onder andere aan welke elektronische gegevensdragers en/of geautomatiseerde werken voor digitaal onderzoek in beslag zijn genomen. Verder maakt de opsporingsambtenaar van politie in BVH of Summ-IT per in beslag genomen elektronische gegevensdragers en/of geautomatiseerde werken een Kennisgeving van Inbeslagneming (KvI) op.[6] In de KvI vermeld de opsporingsambtenaar van politie de gegevens van de eigenaar van de inbeslaggenomen elektronische gegevensdragers en/of geautomatiseerde werken, op grond waarop deze in beslag zijn genomen en de specifieke kenmerken van de inbeslaggenomen elektronische gegevensdragers en/of geautomatiseerde werken. Door het aanmaken van de KvI's hebben alle elektronische gegevensdragers en/of geautomatiseerde werken die in beslag zijn genomen een uniek goednummer. De KvI wordt in het dossier opgeslagen en uitgeprint. De uitgeprinte versie wordt op de in beslag genomen elektronische gegevensdragers en/of geautomatiseerde werken gepakt. Vervolgens worden de elektronische gegevensdragers en/of geautomatiseerde werken bij de digitaal rechercheur van het team digitale opsporing van de eenheid waarbinnen het opsporingsonderzoek valt afgeleverd voor digitaal onderzoek.

8. Digitaal onderzoek

De digitaal rechercheur neemt de inbeslaggenomen elektronische gegevensdragers en/of geautomatiseerde werken in ontvangst voor het uitvoeren van digitaal onderzoek. Allereerst start de digitaal rechercheur met het veiligstellen van alle gegevens die op de elektronische gegevensdragers en/of geautomatiseerde werken zijn opgeslagen. Veiligstellen houdt in dat de gegevens met behulp van forensisch onderzoek programmatuur van de elektronische gegevensdragers en/of geautomatiseerde werken worden gekopieerd. Dit is een forensische kopie wat inhoudt dat de digitaal rechercheur de beschikking heeft over alle gegevens die op het 'bestandsysteem' zijn of waren opgeslagen. Hierdoor kan de digitaal rechercheur ook verwijderde gegevens of delen daarvan weer inzichtelijk maken.

In sommige gevallen lukt het de digitaal rechercheur niet om de gegevens op de elektronische gegevensdragers en/of geautomatiseerde werken veilig te stellen. In dat geval maakt de digitaal rechercheur gebruik van de expertise van het Nederlands Forensisch Instituut (NFI). Betreft het een mobiele telefoon die niet veiliggesteld kan worden, dan maakt de digitaal rechercheur voor het veiligstellen gebruik van de diensten van Forensisch softwarebedrijf 5.1.2.I. In dat geval noteert de digitaal rechercheur in Dashboard dat het veiligstellen niet is gelukt en dat dit door het NFI of 5.1.2.I gebeurt. Vervolgens draagt de digitaal rechercheur de elektronische gegevensdragers en/of geautomatiseerde werken over aan TDO. TDO is de contactpersoon richting NFI en 5.1.2.I en beslist samen met de OvJ of het veiligstellen door het NFI of 5.1.2.I gebeurt. In dat geval worden de elektronische gegevensdragers en/of geautomatiseerde werken fysiek of per post aan het NFI of 5.1.2.I verstrekt. De veiliggestelde gegevens worden op een harde schijf of beveiligde USB-Stick gezet. TDO ontvangt de veiliggestelde gegevens en inbeslaggenomen elektronische gegevensdragers en/of geautomatiseerde werken fysiek of per aangetekende post terug. Indien het de digitaal rechercheur wel lukt om de gegevens veilig te stellen, krijgen de gegevens na het veiligstellen een 'hashwaarde' die identiek is aan de originele dataset. Met de 'hashwaarde' kan de opsporingsambtenaar van politie aantonen dat de veiliggestelde gegevens ongewijzigd zijn. De veiliggestelde gegevens worden door de technisch rechercheur opgeslagen in de Evidence- en Exportmap van de applicatie 5.1.2.I. De Evidencemap wordt door de technisch rechercheur volledig afgesloten om te waarborgen dat de veiliggestelde gegevens in de Evidencemap ongewijzigd blijft. Na het opslaan van de veiliggestelde gegevens stelt de digitaal rechercheur in Dashboard een 'proces-verbaal van veiligstellen' op. In dit proces-verbaal staat de personalia van de eigenaar van de elektronische gegevensdragers en/of geautomatiseerde werken en welke relevante gegevens daarop zijn aangetroffen. Het 'proces-verbaal van veiligstellen' wordt in de Reportmap van 5.1.2.I opgeslagen. Vervolgens start de digitaal rechercheur met het digitaal onderzoek. Voorafgaand aan het digitaal onderzoek heeft de digitaal rechercheur een onderzoeksvraag van de opsporingsambtenaar van politie gekregen. Bijvoorbeeld: 'is deze inbeslaggenomen mobiele telefoon van de verdachte op de plaats delict geweest?'. Op basis van de onderzoeksvraag analyseert de digitaal rechercheur de veiliggestelde gegevens in de Exportmap van 5.1.2.I. De digitaal rechercheur analyseert de gegevens met behulp van verschillende analyseprogrammatuur, zoals 5.1.2.I en 5.1.2.I. Van de resultaten die uit het digitaal onderzoek zijn gekomen wordt een rapport gegenereerd. Dit rapport wordt door de digitaal rechercheur in de Exportmap van 5.1.2.I opgeslagen zodat de tactisch

[6] Art. 94 lid 3 Wetboek van Strafvordering

rechercheur van het tactisch team hiermee verder kan. Ook heeft het onderzoeksteam via deze map toegang tot de veiliggestelde en geanalyseerde gegevens. De inbeslaggenomen elektronische gegevensdragers en/of geautomatiseerde werken worden na het veiligstellen van de gegevens door de digitaal rechercheur teruggebracht naar het onderzoeksteam. Het onderzoeksteam zorgt er vervolgens voor dat de elektronische gegevensdragers en/of geautomatiseerde werken teruggaan naar de eigenaar of worden vernietigd.

9. Tactisch rechercheur
De tactisch rechercheur opent het rapport dat in de Exportmap van [redacted] is opgeslagen. Aan de hand van de resultaten in het rapport probeert de tactisch rechercheur de onderzoekvraag te beantwoorden. Indien de tactisch rechercheur een verdiepingsvraag heeft, neemt hij contact op met de digitaal rechercheur. De digitaal rechercheur beantwoordt de verdiepingsvraag en zet zijn antwoord in een 'proces-verbaal van bevindingen'. Dit proces-verbaal wordt door de digitaal rechercheur in BVH of Summ-IT opgemaakt. Als de tactisch rechercheur de onderzoeksvraag heeft beantwoord stelt hij deze informatie ter beschikking aan het onderzoeksteam zodat zij deze informatie in hun opsporingsonderzoek kunnen gebruiken en aan het onderzoeksdossier kunnen toevoegen.

2. Big data

2a. Als er sprake is van een verwerking van big data, geef een toelichting waarom de verwerking voldoet aan de kenmerken van 'big data'.

Beschrijving van een big dataverwerking:

Niet van toepassing.

2b. Is de big dataverwerking getoetst aan het 'kwaliteitskader big data' opgesteld door de politie en het openbaar ministerie?

- ☐ Ja
- ☐ Nee
- ✓ Niet van toepassing

3. Motivatie hoog risico verwerking

Geef aan waarom sprake is van een hoog risicoverwerking en waarom een GEB nodig is. Licht toe waarom aan twee of meer criteria wordt voldaan.

Antwoord:

Algemeen
De Europese toezichthouder, het European Data Protection Board (EDPB), heeft negen criteria opgesteld om te beoordelen of een verwerking van politiegegevens[7] een hoog privacyrisico oplevert voor de personen over wie een organisatie politiegegevens verwerkt. Als uitgangspunt geldt dat een gegevensverwerking een hoog risicoverwerking is als deze aan twee of meer van de onderstaande criteria voldoet. In dat geval is het uitvoeren van een gegevensbeschermingseffectbeoordeling (GEB) op de verweking noodzakelijk.

Criteria:

1. Beoordelen van mensen op basis van persoonskenmerken
2. Geautomatiseerde beslissingen
3. Stelselmatige en grootschalige monitoring
4. Bijzondere politiegegevens

[7] Art. 1 lid a Wet politiegegevens

5. Grootschalige gegevensverwerkingen
6. Gekoppelde databases
7. Gegevens over kwetsbare personen
8. Gebruik van nieuwe technologieën
9. Blokkering van een recht, dienst of contract

Reden GEB

Een GEB moet worden uitgevoerd als sprake is van een 'hoog risico' verwerking. Daar is hier sprake van, omdat:

- bij het uitvoeren van digitaal onderzoek politiegegevens van zeer persoonlijke aard kunnen worden verwerkt, zoals bijzondere politiegegevens;
- er op grote schaal politiegegevens worden verwerkt;
- het uitvoeren van digitaal onderzoek grote impact op de betrokkenen kan hebben die als kwetsbare personen dienen te worden beschouwd.

4. Politiegegevens

Beschrijf per categorie betrokkene de politiegegevens die worden verwerkt. Geef aan of het algemene of bijzondere politiegegevens zijn. Voeg een dataoverzicht van de applicaties toe als bijlage.

4a. Geef een beschrijving van de betrokkenen en de politiegegevens

Toelichting op onderstaande tabel:
In de tabel is opgenomen welke politiegegevens bij het uitvoeren van digitaal onderzoek worden verwerkt. Dat wil echter niet zeggen dat al deze politiegegevens bij ieder digitaal onderzoek worden verwerkt. De politiegegevens die worden verwerkt is afhankelijk van de gegevens die op de inbeslaggenomen elektronische gegevensdragers en/of geautomatiseerde werken zijn opgeslagen.

Politiegegevens **(Bijvoorbeeld: Naam, geboortedatum, BSN, en rekeningnummer).**	**Type politiegegevens** • **Normaal** • **Bijzonder**	**Categorie van betrokkenen**
Contactgegevens en overige politiegegevens: • Achternaam • Voornamen • Geboortedatum • Nationaliteit • Geslacht • Burgerservicenummer • Feitelijke verblijfplaats • (Historische) GBA-gegevens • Beroep/studie • Werkadres/ schooladres • Burgerlijke staat • Telefoonnummer • Bank-/creditcardnummer • Betaalgegevens • Financiële transacties • Gebruik OV kaart • Kentekenregistratie • Tenaamstelling	Normaal	• Slachtoffer • Verdachte(n) • Overige betrokkenen

Politiegegevens **(Bijvoorbeeld: Naam, geboortedatum, BSN, en rekeningnummer).**	**Type politiegegevens** • **Normaal** • **Bijzonder**	**Categorie van betrokkenen**
• Automatic Number Plate Recognition (ANPR-gegevens) • Aangestraalde Bluetooth sensoren • Automotive gegevens (bijvoorbeeld informatie uit de boordcomputer of een ingebouwd navigatiesysteem) • Een kenmerk dat de relatie tussen de betrokkene en de organisatie aanduidt, zoals: Klantnummer, Polisnummer, Factuurnummer • E-mailadres • E-mailadressen waarmee de betrokkene contact heeft gehad • Message-ID[8] • Belgeschiedenis • Gebruikersnaam/inloggegevens (niet zijnde wachtwoorden) • Vriendenlijst • IP adressen • International Mobile Equipment Identity[9] • International Mobile Subscriber Identity[10] • Locatiegegevens <u>In geval van een rechtspersoon</u> • Handelsnaam • Adres/ Postadres • vestigingsplaats		
Contactgegevens en overige politiegegevens: • Achternaam • Voorvoegsel(s) • Voorletter(s) • Dienstnummer • Functie	Normaal	• Algemene opsporingsambtenaren • Technisch rechercheur • Tactisch rechercheur

[8] Message-ID is een uniek nummer van een e-mailbericht.
[9] International Mobile Equipment Identity is een uniek nummer dat toebehoort aan een telefoon.
[10] International Mobile Subscriber Identity is een identificatie van aan SIM kaart geregistreerde gebruiker.

Politiegegevens **(Bijvoorbeeld: Naam, geboortedatum, BSN, en rekeningnummer).**	**Type politiegegevens** • **Normaal** • **Bijzonder**	**Categorie van betrokkenen**
• Handtekening		
Contactgegevens en overige politiegegevens: • Titel • Achternaam • Voornaam	Normaal	• Behandelend OvJ
Contactgegevens en overige politiegegevens: • RC-nummer	Normaal	• RC
Geluid en/of beeldmateriaal • Camerabeelden waarop betrokkene(n) herkenbaar in beeld zijn. • Voicemailberichten	Normaal, bijzonder	• Slachtoffer • Verdachte(n) • Overige betrokkenen
Sociale media • Gebruikersnaam/inlog-gegevens (niet zijnde wachtwoorden) • geplaatste en verwijderde berichten, afbeeldingen, video's, blogs en advertenties • Verzonden en ontvangen berichten • Vriendenlijst/contactenlijst • Reacties op geplaatste berichten	Normaal, bijzonder	• Slachtoffer • Verdachte(n) • Overige betrokkenen
Berichten • Ontvangen e-mailberichten • Verzonden e-mailberichten • conceptenberichten • berichten in de prullenbak • Voicemailberichten	Normaal, bijzonder	• Slachtoffer • Verdachte(n) • Overige betrokkenen

Politiegegevens (Bijvoorbeeld: Naam, geboortedatum, BSN, en rekeningnummer).	Type politiegegevens • Normaal • Bijzonder	Categorie van betrokkenen
• Inhoud van SMS, MMS, EMS en Faxberichten		
Bijzondere politiegegevens: • Foto's, video's en berichten waaruit bijzondere politiegegevens blijken • Camerabeelden ter identificatie van betrokkenen. • Medisch ID	Bijzonder	• Slachtoffer • Verdachte(n) • Overige betrokkenen

4b. (Technische) hulpmiddelen
Beschrijf op welke wijze en met gebruikmaking van welke (technische) middelen de politiegegevens worden verwerkt. Benoem of sprake is van een handmatig of geautomatiseerd proces.

Toelichting:

De onderstaande (technische) middelen worden binnen de verwerking gebruikt.	
(Technische) middelen	**Toelichting**
Applicaties en systemen die gebruikt worden als verwerkingssysteem of bron van informatie ten behoeve van de verwerking 'Uitvoeren digitaal onderzoek'.	• Servicemodule • Artikel 12 Wpg mailbox • BVH • Summ-IT • 5.1.2.i • Dashboard • 5.1.2.i • 5.1.2.i • OxygenEncase • FTK • Troi-applicaties

5. Gegevensstroom

Beschrijf de gegevensstroom aan de hand van de verschillende stadia van een verwerking. Benoem tevens de middelen en systemen die voor de verwerking gebruikt worden. Wanneer er een gegevensstroomschema of werkprocesbeschrijving beschikbaar is, kun je deze als bijlage toevoegen.

5a. Beschrijf de stadia van de gegevensstroom

Stadia verwerking	Beschrijf de handelingen van de verwerking	Middelen, landelijke systemen, EBO's
Start van de verwerking, herkomst van de gegevens, wijze van verkrijging	De verwerking 'Uitvoeren digitaal onderzoek' begint vanaf het moment dat elektronische gegevensdragers en/of geautomatiseerde werken door de opsporingsambtenaar van politie in beslag worden genomen voor digitaal onderzoek.	• BVH • Summ-IT
Vastleggen, ordenen, structureren, bijwerken of wijzigen, gebruiken, raadplegen, combineren, afschermen	• Er is via een van de verschillende kanalen een melding binnengekomen van een vermoedelijke wetsovertreding waarvoor doorzoeking ter inbeslagname noodzakelijk is; **<u>Doorzoeking ter inbeslagname: openbare ruimte:</u>** • Zie stappen bij 'vervolg'. **<u>Doorzoeking ter inbeslagname: gesloten ruimte, niet zijnde woonruimte</u>** • Na de melding vraagt de opsporingsambtenaar van politie mondeling een machtiging tot binnentreden aan bij de HOvJ; • De HOvJ maakt een machtiging tot binnentreden op; • Machtiging tot binnentreden wordt aan het onderzoeksdossier toegevoegd (Zie verder stappen bij 'vervolg'); **<u>Doorzoeking ter inbeslagname: gesloten ruimte, zijnde woonruimte</u>** • Na de melding wordt er een 'Aanvraag proces-verbaal binnentreden' opgemaakt en doorgestuurd naar de RC. Dit is de aanvraag voor de machtiging tot binnen treden. (Zie verder stappen bij 'vervolg';	• BVH • Summ-IT • 5.1.2.i • Dashboard • 5.1.2.i • 5.1.2.i • Oxygen • Troi-applicaties

	<u>Vervolg:</u> • Er volgt een briefing of kort overleg over de melding; • De plaats wordt doorzocht op aanwezigheid van elektronische gegevensdragers en/of geautomatiseerde werken die voor digitaal onderzoek inbeslaggenomen moeten worden; • De opsporingsambtenaar van politie neemt de inbeslaggenomen elektronische gegevensdragers en/of geautomatiseerde werken mee naar het politiebureau; • De opsporingsambtenaar van politie maakt in Summ-IT een 'proces-verbaal van doorzoeking' en in BVH of Summ-IT per inbeslaggenomen elektronische gegevensdragers en/of geautomatiseerde werken een KvI op; • De opsporingsambtenaar van politie print de KvI's uit en plakt deze op de inbeslaggenomen elektronische gegevensdragers en/of geautomatiseerde werken waarvoor de KvI is opgemaakt; • De opsporingsambtenaar van politie levert de inbeslaggenomen elektronische gegevensdragers en/of geautomatiseerde werken af bij de digitaal rechercheur van de eenheid waarbinnen het opsporingsonderzoek valt; • De digitaal rechercheur start met het veiligstellen van de gegevens op de elektronische gegevensdragers en/of geautomatiseerde werken; • De veiliggestelde gegevens slaat de digitaal rechercheur op in de Evidence- en Exportmap van 5.1.2.1; • De digitaal rechercheur sluit de Evidencemap; • Vervolgens maakt de digitaal rechercheur een 'proces-verbaal van veiligstellen' op in Dashboard. Het proces-verbaal wordt door de digitaal	

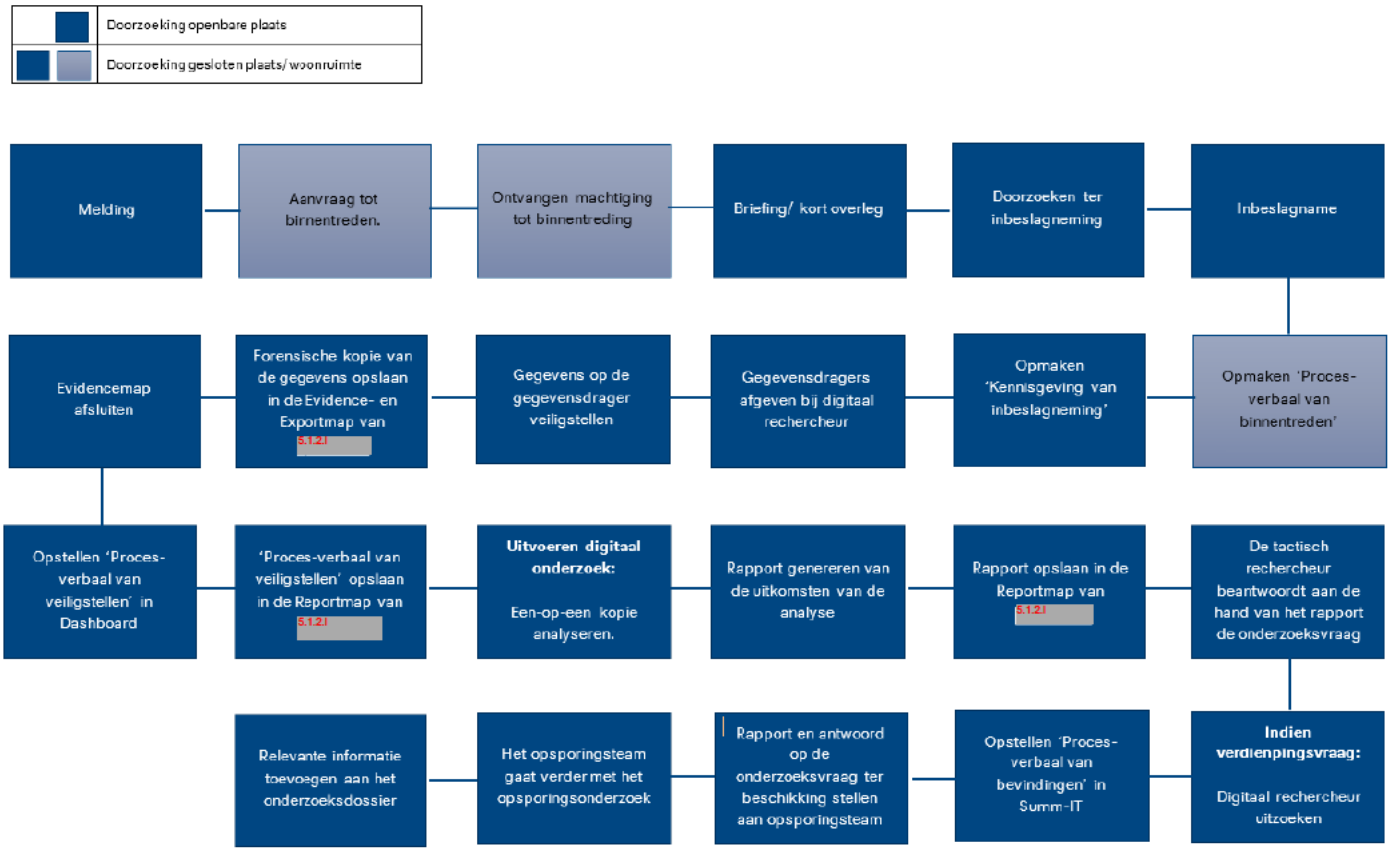
	rechercheur in de Reportmap van 5.1.2.i opgeslagen; • Start digitaal onderzoek: De veiliggestelde gegevens worden met behulp van forensisch onderzoek programmatuur geanalyseerd op informatie die de onderzoeksvraag kan beantwoorden; • De digitaal rechercheur genereert een rapport van de resultaten die uit de analyse naar voren zijn gekomen; • Het rapport wordt opgeslagen in de Reportmap van 5.1.2.i; • De tactisch rechercheur heeft via de Reportmap van 5.1.2.i beschikking over het rapport en analyseert de resultaten. • Bij een verdiepingsvraag neemt de tactisch rechercheur contact op met de digitaal rechercheur; • De digitaal rechercheur geeft antwoord op de verdiepingsvraag in het 'proces-verbaal van bevindingen'. Dit proces-verbaal maakt de digitaal rechercheur in het politiesysteem Summ-IT. • Na het analyseren van de resultaten in het rapport en het beantwoorden van de verdiepingsvraag worden de politiegegevens via de reportmap van 5.1.2.i ter beschikking gesteld aan de opsporingsambtenaar van politie van het onderzoekstem die met het onderzoek is belast.	
Resultaten, producten van de verwerking	• Aanvraag proces-verbaal binnentreding • Proces-verbaal van doorzoeking • KvI • Images[11] van de veiliggestelde gegevens • Proces-verbaal van veiligstellen • Rapport resultaten van analyse • Proces-verbaal van bevinding	• BVH • Summ-IT • 5.1.2.i

[11] Een image is een kopie van alle bestanden, mappen en programma's van op de elektronische gegevensdrager en/of geautomatiseerde werken.

Verwijderen van gegevens (meer gedetailleerd in vraag 9)	Binnen BVH worden politiegegevens 5 jaar na eerste verwerking automatisch verwijderd. Verwijderen houdt in de praktijk in dat politiegegevens als het ware achter een 'schot' worden geplaatst en alleen benaderbaar zijn via een poortwachter, in opdracht van het bevoegd gezag bij hernieuwd verwerken. Politiegegevens binnen Summ-IT worden niet automatisch verwijderd. Om de gegevens te verwijderen is het van belang dat de opsporingsambtenaar van politie het opsporingsonderzoek handmatig op status 'voltooid' zet. Politiegegevens in 5.1.2.i worden handmatig verwijderd. Drie maanden na het afronden van een digitaal onderzoek ontvangt de teamleider van het opsporingsonderzoek een mail met de vraag of de gegevens in 5.1.2.i kunnen worden verwijderd. Bij akkoord worden de Evidence- en Reportmap op tape gezet en gearchiveerd. De Exportmap wordt verwijderd. Na het verwijderen zit de map nog 28 dagen in een prullenbak, maar doordat de autorisaties na het verwijderen direct worden ingetrokken is het voor de ambtenaren van politie die toegang hadden tot de politiegegevens niet meer mogelijk om deze terug te halen. Na de 28 dagen zijn de politiegegevens in de Exportmap definitief verwijderd.	• BVH • Summ-IT • 5.1.2.i
Uitwijkvoorziening in geval continuïteit	BVH, Summ-IT en 5.1.2.i hebben een back-up voorziening.	• BVH • Summ-IT • 5.1.2.i
Vernietigen	**BVH** Het politiesysteem BVH is ingericht volgens de bewaar- en vernietigingstermijnen uit artikel 8 Wpg. In de praktijk worden politiegegevens die ten behoeve van de uitvoering van de dagelijkse politietaak zijn verwerkt niet vernietigd. De politiegegevens worden bewaard omdat deze mogelijk nog van belang kunnen zijn voor cold case onderzoek. **Summ-IT** Het politiesysteem Summ-IT is ingericht volgens de bewaar- en vernietigingstermijnen uit artikel 9 Wpg. Zodra een opsporingsonderzoek door de opsporingsambtenaar van politie op afgehandeld wordt gezet, beginnen de bewaar- en vernietigingstermijnen te	• BVH • Summ-IT • 5.1.2.i

	lopen. Een onderzoeksdossier wordt door de ambtenaar van politie pas op afgehandeld gezet na een afdoeningsbericht van het OM. In de praktijk komt het structureel voor dat de ambtenaar van politie door het OM niet op de hoogte wordt gebracht van een door het OM afgesloten dossier. Als gevolg hiervan blijven politiegegevens op status 'actief' en gaan de bewaartermijnen niet lopen. Als een onderzoeksdossier wel op afgehandeld wordt gezet worden de politiegegevens na het verstrijken van de bewaartermijn niet vernietigd. De gegevens worden na de bewaartermijn achter een schot geplaatst en zijn hierdoor alleen door functioneel beheer benaderbaar. Functioneel beheer kan de inhoud van het onderzoeksdossier niet bekijken, maar heeft de mogelijkheid om het onderzoek te heropenen. **Pandora** Het is vooraf niet te bepalen wanneer een strafrechtelijk onderzoek definitief is afgerond, omdat er in een strafrechtelijk onderzoek één of meerdere (onbekende) verdachten kunnen zitten. Bijvoorbeeld: als X onherroepelijk is veroordeeld voor drugshandel, betekent dat niet per definitie dat de gegevens niet meer nodig zijn voor het opsporingsonderzoek. Deze gegevens kunnen namelijk nog noodzakelijk voor het oprollen van de hele drugsorganisatie waar X onderdeel van was. Om deze reden worden politiegegevens die uit het digitaal onderzoek zijn verkregen en in 5.1.2.i zijn opgeslagen pas vernietigd als het geplaagde strafbare feit is verjaard. De politiegegevens worden tot die tijd op tape gezet en gearchiveerd. Als de politiegegevens op tape staan, zijn deze niet meer raadpleegbaar. In 5.1.2.i is dan alleen te zien welke onderzoek het betreft, wie het onderzoek in 5.1.2.i heeft aangemaakt, wanneer het onderzoek is gearchiveerd etc. Alleen functioneel beheer kan de politiegegevens met toestemming van het bevoegd gezag weer inzichtelijk maken voor de operatiën.	

5b. Overzicht van de gegevensstroom:



5c. Welke werkprocessen zijn beschikbaar om inzicht te krijgen in de verwerking?

Geef inzicht in de werkprocessen uit het bedrijfsreferentiemodel (hierna: BRM) die betrekking hebben op de verwerking.

De volgende werkprocessen in de bedrijfsarchitectuur zijn te koppelen aan de verwerking:

Te koppelen werkprocessen:

- Coördineren digitaal onderzoek
- Uitvoeren digitaal (forensisch) onderzoek
- Uitvoeren eenvoudig digitaal (forensisch) onderzoek
- Onderzoeken plaats delict (digitaal)

5d. Eigen beheerde omgeving

Als er gebruik gemaakt wordt van lokale 'eigen beheerde omgevingen' (EBO's) vul je de volgende gegevens in:

Naam EBO	Doel van de EBO	Eenheid die een EBO beheert	Eigenaar
5.1.2.i	5.1.2.i	5.1.2.e	5.1.2.e

6. Doel van de verwerking

Beschrijf het doel van de (voorgenomen) gegevensverwerking en eventuele andere doelen die gerelateerd zijn aan de verwerking. Beschrijf waar de verwerking concreet voor bedoeld is en waar het op gericht is.

Verwerking	Doel van de verwerking
Uitvoeren digitaal onderzoek	Het doel van de gegevensverwerking is om informatie te verkrijgen uit gegevensdragers en/of geautomatiseerde werken die richting kan geven aan het opsporingsonderzoek en/of in de rechtszaak als bewijslast tegen de verdachte(n) gebruikt kan worden.

7. Betrokken partijen en hun belangen

Benoem welke externe partijen betrokken zijn bij de (voorgenomen) gegevensverwerking. Het gaat om hun rol en belang als ontvanger, verstrekker of verwerker. Beschrijf de politiegegevens die aan deze partijen worden verstrekt. Voor de indeling van de externe partijen is gebruik gemaakt van paragraaf 3 van de Wpg.

Partij	Rol en belang partijen	Politiegegevens
Officier van Justitie	**Ontvanger van politiegegevens** De opsporingsambtenaar van politie treedt bij het uitvoeren van digitaal onderzoek op onder het gezag van de OvJ, vertegenwoordiger van het OM. Het OM ontvangt politiegegevens voor zover zij deze behoeven in verband met hun gezag of zeggenschap over de politie of voor andere krachtens de wet aan het OM opgedragen taken.	Gewone en bijzondere politiegegevens
Nederlands Forensisch Instituut (NFI)	**Ontvanger en verstrekker van politiegegevens** De deskundigen van het NFI kunnen op verzoek van de opsporingsambtenaar van politie helpen bij het veiligstellen van inbeslaggenomen elektronische gegevensdragers en/of geautomatiseerde werken. De opsporingsambtenaar van politie verstrekt politiegegevens aan het NFI ten behoeve van de uitvoering van zijn taken met het oog op de waarheidsvinding in strafzaken, het leveren van een bijdrage aan de handhaving van de internationale en nationale rechtsorde of veiligheid, de ondersteuning bij de hulpverleningstaak van de politie en het leveren van een dienst of	Gewone en bijzondere politiegegevens

	product. In dit geval ontvangt het NFI de inbeslaggenomen elektronische gegevensdragers en/of geautomatiseerde werken met daarop de politiegegevens die zij met het oog op waarheidsvinding in strafzaken kunnen veiligstellen.	
5.1.2.i	**Ontvanger van politiegegevens** Forensisch softwarebedrijf 5.1.2.i is een organisatie die software ontwikkelt voor het veiligstellen van gegevens op mobiele telefoons. De politie maakt van de diensten van 5.1.2.i gebruik op het moment dat het de digitaal rechercheur van de politie of het NFI niet lukt om gegevens op de inbeslaggenomen mobiele telefoon veilig te stellen. 5.1.2.i is gevestigd in 5.1.2.i en ontvangt de inbeslaggenomen mobiele telefoons van de politie om deze vervolgens veilig te kunnen stellen.	Gewone en bijzondere politiegegevens
5.1.2.i	**Ontvanger van politiegegevens** 5.1.2.i is een organisatie die beëdigde tolken in dienst heeft. De opsporingsambtenaar van politie maakt voor het vertalen van teksten en/of geluidsopnames gebruik van tolken die werkzaam zijn bij deze organisatie.	Gewone en bijzondere politiegegevens De tolk die de teksten en/of geluidsopnames vertaalt krijgt geen politiegegevens toegestuurd, maar krijgt inloggegevens om op het politiebureau de teksten en/of geluidsopnames te kunnen beluisteren en vertalen.

8. Verwerkingslocaties

Geef aan in welke landen de verwerking plaatsvindt. In het geval van een doorgifte aan een derde land of internationale organisatie, geef aan om welke het gaat.

Geef aan waar de verwerking plaatsvindt:

✓ Nederland
✓ overige lidstaten binnen de EU, namelijk: 5.1.2.i
☐ doorgifte aan een derde land of internationale organisatie:

Antwoord:

In sommige gevallen lukt het de digitaal rechercheur niet om de gegevens die op een mobiele telefoon staan veilig te stellen. In dat geval maakt de politie gebruik van de diensten van forensisch softwarebedrijf 5.1.2.i . 5.1.2.i ontwikkelt software voor het veiligstellen van gegevens op mobiele telefoons en is gevestigd in 5.1.2.i . In

opdracht van de politie stelt 5.1.2.i de gegevens op de inbeslaggenomen mobiele telefoons veilig. De inbeslaggenomen mobiele telefoons worden in sommige gevallen door de ambtenaar van politie bij 5.1.2.i afgeleverd of aangetekend verstuurd via de bezorgdiensten van DPD of PostNL. De veiliggestelde gegevens worden na het veiligstellen door 5.1.2.i op een harde schijf of USB-stick gezet en tezamen met de inbeslaggenomen elektronische gegevensdragers en/of geautomatiseerde werken fysiek of per aangetekende post teruggestuurd naar TDO.

9. Verwerkingstermijnen

Beschrijf hoe de verwerkingstermijnen in de praktijk worden gehanteerd. Het gaat om de feitelijke hantering van de verwerkingstermijnen. Beschrijf hierbij ook hoe de gegevens verwijderd, vernietigd en gearchiveerd worden. Geef aan wie deze handelingen uitvoert.

Antwoord:

Verwerkings- en bewaartermijn artikel 8 Wpg (voornamelijk in BVH)

De verwerkingstermijn is de termijn waarbinnen politiegegevens zich in de operationele omgeving bevinden en door de opsporingsambtenaar van politie verwerkt mogen worden ten behoeve van de uitvoering van de dagelijkse politietaak[12] Politiegegevens die ten behoeve van de uitvoering van de dagelijkse politietaak zijn verwerkt mogen maximaal vijf jaar verwerkt worden, te rekenen vanaf de datum van eerste verwerking. Het eerste jaar zijn de politiegegevens vrij beschikbaar. [13] Vervolgens zijn de politiegegevens gedurende vier jaar beschikbaar voor geautomatiseerde vergelijking[14] en voor het in combinatie verwerken.[15] Na de vijf jaar moeten de gegevens worden verwijderd. In de praktijk betekent dit dat de politiegegevens als het ware achter een schot wordt geplaats en alleen benaderbaar zijn via een poortwachter in opdracht van het bevoegd gezag. Vijf jaar na verwijdering moeten de politiegegevens worden vernietigd. In de praktijk worden politiegegevens die ouder zijn dan tien jaar niet vernietigd op grond van het Kamerstuk 29628, nr. 859. In het kamerstuk wordt aangegeven dat de korpschef de huidige bewaartermijnen voor politiegegevens te kort vindt voor cold case onderzoeken. Om die reden heeft de korpschef besloten de politiegegevens ten behoeve van cold case onderzoeken niet structureel te vernietigen. De Minister van Justitie en Veiligheid geeft in het kamerstuk aan achter deze keuze van de korpschef te staan. Het kamerstuk heeft waarde, maar is geen wetgeving of 'vrijbrief' om (structureel) buiten de wettelijke bewaartermijnen zoals opgenomen in de Wpg te gaan. Zodra de bewaartermijn is verstreken is er geen grondslag meer om de politiegegevens te verwerken en is er sprake van onrechtmatige gegevensverwerking als deze gegevens nog worden bewaard.

Verwerkings- en bewaartermijn artikel 9 Wpg (voornamelijk in Summ-IT)

Politiegegevens die door de opsporingsambtenaar van politie worden verwerkt ten behoeve van het opsporingsonderzoek in een bepaald geval,[16] worden verwerkt voor zolang dit noodzakelijk is voor het opsporingsonderzoek. In geval van een opsporingsonderzoek dat heeft geleid tot vervolging zal dat pas zijn nadat de rechter ten aanzien van de zaak onherroepelijk heeft beslist. De gegevens zijn tot die tijd nodig voor het geval de OvJ, de RC of de rechter ter zitting nader onderzoek verlangt. Betreft het een onopgelost onderzoek, dan blijven de gegevens nodig voor het doel van onderzoek en mogen de gegevens worden verwerkt tot uiterlijk het moment waarop de feiten zijn verjaard. Als de politiegegevens niet meer noodzakelijk zijn voor het doel waarvoor ze zijn verkregen moeten zij op grond van de Wpg worden verwijderd of mogen zij gedurende een periode van maximaal een half jaar verwerkt worden om te bezien of bepaalde politiegegevens mogelijk noodzakelijk zijn voor de politietaak en daartoe voor een ander doel verwerkt kunnen worden. Op de verwijderingstermijn volgt de bewaartermijn. Verwijderde politiegegevens moeten voor de duur van vijf jaar worden bewaard, te rekenen vanaf de datum van verwijdering.[17] In de praktijk wordt een opsporingsonderzoek dat door de opsporingsambtenaar van politie is afgehandeld en aan het OM is overhandigd in Summ-IT op status 'voltooid' gezet. Dit betreft een politionele afsluiting wat inhoudt dat de politie aangeeft het opsporingsonderzoek afgerond te hebben. De politiegegevens bevinden zich bij een politionele afsluiting nog in de operationele omgeving, maar er blijven dan nog maar een beperkt aantal opsporingsambtenaren van politie die bij het opsporingsonderzoek betrokken waren aan het

[12] Artikel 8 lid 1 Wet politiegegevens
[13] Artikel 8 lid 1 Wet politiegegevens
[14] Artikel 8 lid 2 Wet politiegegevens
[15] Artikel 8 lid 3 Wet politiegegevens
[16] Art. 9 lid 1 Wet Politiegegevens
[17] Artikel 14 lid 1 Wpg

onderzoek gekoppeld. Dit zodat zij eventuele vragen van de OvJ, RC of rechter met betrekking tot het opsporingsonderzoek kunnen beantwoorden. De rest van het onderzoeksteam wordt gedeactiveerd/ gedeautoriseerd. De bewaartermijn van de politiegegevens start in de praktijk vanaf het moment dat het opspringsonderzoek door de opsporingsambtenaar van politie in Summ-IT op afgehandeld is gezet. De opsporingsambtenaar van politie zet een opsporingsonderzoek pas op afgehandeld na een afdoeningsbericht van het OM. Met het afdoeningsbericht laat het OM de opsporingsambtenaar van politie weten dat de verdachte(n) door het OM is/zijn vervolgd, de strafzaak onherroepelijk is geworden, of enige vorm van sepot en het dossier daarmee definitief voltooid is en de opsporingsambtenaar van politie het dossier daarmee in Summ-IT kan afsluiten. In de praktijk komt het structureel voor dat de opsporingsambtenaar van politie niet op de hoogte wordt gebracht van een door het OM afgesloten dossier. Als een onderzoeksdossier wel op afgehandeld wordt gezet worden de politiegegevens na het verstrijken van de bewaartermijn niet vernietigd. De gegevens worden na de bewaartermijn achter een schot geplaatst en zijn hierdoor alleen door functioneel beheer benaderbaar. Functioneel beheer kan de inhoud van het onderzoeksdossier niet bekijken, maar heeft de mogelijkheid om het onderzoek te heropenen. Als dat gebeurt kan er weer in het onderzoek worden gewerkt. Doordat de politiegegevens na het verstrijken van de bewaartermijn niet worden vernietigd worden de politiegegevens langer verwerkt dan door de wetgever is bepaald. Er is sprake van een onrechtmatige gegevensverwerking.

5.1.2.I

Politiegegevens die uit het digitaal onderzoek zijn verkregen en in 5.1.2.I zijn opgeslagen worden verwerkt voor zolang dit noodzakelijk is voor het opsporingsonderzoek. Als de politiegegevens niet meer noodzakelijk zijn voor het doel waarvoor ze zijn verkregen moeten zij op grond van de Wpg worden verwijderd of mogen zij gedurende een periode van maximaal een half jaar verwerkt worden om te bezien of bepaalde politiegegevens mogelijk noodzakelijk zijn voor de politietaak en daartoe voor een ander doel verwerkt kunnen worden. In de praktijk ontvangt de teamleider van het opsporingsonderzoek, drie maanden na het afronden van een digitaal onderzoek een mail met de vraag of de gegevens in 5.1.2.I kunnen worden verwijderd. Bij akkoord wordt de Exportmap verwijderd. Na het verwijderen zit de map nog 28 dagen in een prullenbak, maar doordat de autorisaties na het verwijderen direct worden ingetrokken is het voor de ambtenaren van politie die toegang hadden tot de politiegegevens niet meer mogelijk om deze terug te halen. Na de 28 dagen zijn de politiegegevens in de Exportmap definitief verwijderd. De Evidence- en Reportmap worden op tape gezet en gearchiveerd. Als de politiegegevens op tape staan, zijn deze niet meer raadpleegbaar. In 5.1.2.I is dan alleen te zien welk onderzoek het betreft, wie het onderzoek in 5.1.2.I heeft aangemaakt, wanneer het onderzoek is gearchiveerd etc. Alleen functioneel beheer kan de politiegegevens met toestemming van het bevoegd gezag weer inzichtelijk maken voor de operatiën. De politiegegevens die uit het digitaal onderzoek zijn verkregen worden vernietigd als het gepleegde strafbare feit is verjaard.

10. Juridisch en beleidsmatig kader

Benoem de wet- en regelgeving en beleid die een rol spelen voor de (voorgenomen) gegevensverwerking. De Wpg kan hier weggelaten worden tenzij er een bijzondere situatie aan de orde is.

Juridisch en/of beleidsmatigkader
Politiewet 2012
Besluit politiegegevens
Wetboek van Strafvordering
Aanwijzing inbeslagneming (Artikel 94 Sv)
Wet politiegegevens (Wpg)

11. Rechten van betrokkenen

In iedere eenheid worden de verzoeken voor rechten van betrokkenen behandeld door de privacydesk. Geef aan hoe de verwerkingsverantwoordelijke zorgdraagt voor de landelijke uitvoering van rechten betrokkene voor deze verwerking.

Uitvoering rechten betrokkene	Ja	Nee	Toelichting
De portefeuille beschikt over een landelijk protocol om een verzoek voor rechten betrokkene uniform te behandelen, voor de Verwerkingen die onder diens verantwoordelijkheid vallen.	X		
De verwerkingsverantwoordelijke heeft een ingericht proces dat aansluit op de privacy desk	X		
De systemen zijn in staat om bijv. data te verwijderen of inzage te verlenen	X		
De verwerkingsverantwoordelijke is ingesteld om te voldoen aan het recht op informatie aan de betrokkene in o.a. een toegankelijke vorm.	X		

B. Beoordeling rechtmatigheid gegevensverwerking

Beoordeel aan de hand van de feiten zoals vastgesteld in onderdeel A of de (voorgenomen) gegevensverwerking rechtmatig is. Het gaat hier om de beoordeling van de juridische rechtsgrond, noodzaak en doelbinding van de gegevensverwerking. Beoordeel tevens de wijze waarop invulling wordt gegeven aan de rechten van de betrokkenen.

12. Wettelijke doeleinden

Bepaal op welke wettelijke doeleinden (politietaken) de gegevensverwerking is gericht en motiveer waarom deze verwerking onder de gekozen wettelijke doeleinde valt. Deze doeleinden moeten aan wettelijke voorwaarden voldoen, beoordeel hoe aan deze voorwaarden wordt voldaan.
De wettelijke doeleinden zijn:

- Artikel 8 Wpg (uitvoering van de dagelijkse politietaak)
- Artikel 9 Wpg (onderzoek i.v.m. de handhaving van de rechtsorde in een bepaald geval)
- Artikel 10 Wpg (inzicht betrokkenheid van personen bij:
  - a) het beramen of plegen van misdrijven;
  - b) bepaalde ernstige bedreigingen van de rechtsorde;
  - c) ernstige schending van de openbare orde.)
- Artikel 12 Wpg (informanten)
- Artikel 13 Wpg (ondersteunende taken, schriftelijke vastlegging vereist)
- Artikel 22 Wpg (wetenschappelijk onderzoek en statistiek)
- Artikel 25-27 Wpg Rechten van betrokkene

Wettelijke doeleinden	Toetsing
Artikel 9 Wet politiegegevens	De politiegegevens worden door de opsporingsambtenaar van politie verwerkt ten behoeve van een opsporingsonderzoek in een bepaald geval.[18] Het opsporingsonderzoek is gericht op de vaststelling van een verdenking. Het uitvoeren van digitaal onderzoek kan bijdragen aan de vaststelling daarvan. De bevoegdheid tot inbeslagneming van elektronische gegevensdragers en/of geautomatiseerde werken voor het uitvoeren van digitaal onderzoek is voor de opsporingsambtenaar van politie geregeld in de artikelen 95 en 96 Sv. Om beslag mogelijk te kunnen maken heeft de opsporingsambtenaar van politie de steunbevoegdheid[19] om een plaats ter inbeslagname te doorzoeken. De grondslag hiervoor is gelegen in de artikelen 96b, 96c, 97 en 110 Sv.

[18] Artikel 9 lid 1 Wet politiegegevens
[19] Een steunbevoegdheid kan worden omschreven als een bevoegdheid die bedoeld is om de uitoefening van een andere bevoegdheid, in dit geval het uitvoeren van digitaal onderzoek, mogelijk te maken.

13. Bijzondere politiegegevens

In deel A is beschreven of en welke bijzondere politiegegevens worden verwerkt. Het verwerken van bijzondere politiegegevens gebeurt uitsluitend als dit onvermijdelijk is voor het doel van de verwerking, een aanvulling is op de verwerking van andere politiegegevens betreffende de persoon en de gegevens afdoende zijn beveiligd, art. 5 Wpg.

Beoordeel of de verwerkte bijzondere politiegegevens voldoen aan de vereisten van artikel 5 Wpg:

Wettelijke eis	Toetsing
De aangegeven te verwerken bijzondere politiegegevens zijn onvermijdelijk voor het doel	Bij het uitvoeren van digitaal onderzoek worden elektronische gegevensdragers en/of geautomatiseerde werken volledig uitgelezen. Na het uitlezen heeft de digitaal rechercheur een forensische kopie van alle gegevens die op het 'bestandsysteem' van de uitgelezen elektronische gegevensdragers en/of geautomatiseerde werken zijn of waren opgeslagen. Het kan zijn dat hierdoor politiegegevens worden verwerkt waaruit politieke opvattingen, gezondheid, lidmaatschap van een vakbond, seksueel gedrag, seksuele gerichtheid en religieuze of levensbeschouwelijke opvattingen blijken. Enerzijds kunnen deze bijzondere politiegegevens ten behoeve van het opsporingsonderzoek gericht worden verwerkt, Bijvoorbeeld omdat de digitaal rechercheur op zoek is naar kinderporno. Anderzijds als 'bijvangst' omdat deze gegevens op de elektronische gegevensdragers en/of geautomatiseerde werken zijn of waren opgeslagen. In beide gevallen is het verwerken van bijzondere politiegegevens onvermijdelijk voor het doel. Het doel van digitaal onderzoek is om informatie te verkrijgen die richting kan geven aan het opsporingsonderzoek en/of in de rechtszaak als bewijslast tegen de verdachte(n) gebruikt kan worden. Hiervoor is het noodzakelijk dat de gehele elektronische gegevensdragers en/of geautomatiseerde werken worden uitgelezen, ook zodat zowel belastende als ontlastende informatie verkregen kan worden. Door in de forensische kopie veranderingen aan te brengen kan de indruk ontstaan dat ontlastende informatie is verwijderd (of belastende informatie is toegevoegd), dus wijzigingen moeten worden voorkomen.
De te verwerken bijzondere politiegegevens zijn een aanvulling op de andere politiegegevens	Bij het uitvoeren van digitaal onderzoek worden 'gericht' of als 'bijvangst' bijzondere politiegegevens verwerkt. Bijzondere politiegegevens worden te allen tijde in aanvulling op gewone politiegegevens verwerkt en nooit uitsluitend.
De te verwerken bijzondere politiegegevens zijn afdoende beveiligd	De bijzondere politiegegevens zijn afdoende beveiligd. Alleen geautoriseerde ambtenaren van politie die betrokken zijn bij het opsporingsonderzoek hebben toegang tot de bijzondere politiegegevens. Om bij deze gegevens te komen moet de ambtenaar van politie inloggen middels multifactorauthenticatie.

14. Verdere verwerkingen

Politiegegevens kunnen verder worden verwerkt nl. in combinatie met elkaar en kunnen ter beschikking worden gesteld mits wordt voldaan aan de wettelijke vereisten en als men daartoe geautoriseerd is volgens artikel 15 en 15a Wpg.

Beoordeel in geval van een verdere verwerking of aan de wettelijke vereisten is voldaan:

Verdere verwerkingen	Toetsing
Artikel 9 lid 3 Wpg	Op grond van artikel 9 lid 3 Wpg mogen politiegegevens die ten behoeve van een opsporingsonderzoek in een bepaald geval zijn verwerkt, ter beschikking worden gesteld voor verdere verwerking ten behoeve van bepaalde andere doelen binnen de politietaak. In geval van de verwerking ' Uitvoeren digitaal onderzoek' is er geen sprake van verdere verwerking van politiegegevens.

15. Verstrekkingen aan externe partijen

De Wpg is een gesloten systeem voor de verstrekkingen aan partijen buiten het politiedomein. Per externe partij moet de verstrekking worden beoordeeld.

Beoordeel of de verstrekkingen aan externe partijen voldoen aan de wettelijke vereisten.

- Verstrekking aan gezagsdragers: artikel 16 Wpg
- Verstrekking aan inlichtingendiensten: artikel 17 Wpg
- Verstrekking aan derden structureel: artikel 18 Wpg
- Verstrekking aan derden incidenteel: artikel 19 Wpg
- Verstrekking aan derden structureel voor een samenwerkingsverband: artikel 20 Wpg
- Rechtstreekse verstrekking: artikel 23 Wpg
- Rechtstreekse verstrekking aan inlichtingen- en veiligheidsdiensten: artikel 24 Wpg

Externe partij	Toelichting
Officier van Justitie	Het opsporen van strafbare feiten behoort tot de strafrechtelijke handhaving van de rechtsorde. In dat geval treedt de ambtenaar van politie op onder het gezag van de OvJ,[20] vertegenwoordiger van het OM. Op grond van artikel 16 lid 1 sub a Wpg is de ambtenaar van politie verplicht om politiegegevens te verstrekken aan leden van het OM voor zover zij deze behoeven in verband met hun gezag of zeggenschap over de politie of voor andere krachtens de wet aan het OM opgedragen taken.
Nederlands Forensisch Instituut (NFI)	Het NFI is een internationaal kennis- en expertisecentrum voor forensisch onderzoek. Op verzoek van de opsporingsambtenaar van politie kan het NFI ondersteunen bij het veiligstellen van inbeslaggenomen elektronische gegevensdragers en/of geautomatiseerde werken. TDO verstrekt politiegegevens aan het NFI op grond van artikel 4:3 lid 1 sub r Besluit politiegegevens ten behoeve van de uitvoering van zijn taken met het oog op de waarheidsvinding in strafzaken, het leveren van een bijdrage aan de

[20] Artikel 12 lid 1 Politiewet 2012

Externe partij	Toelichting
	handhaving van de internationale en nationale rechtsorde of veiligheid, de ondersteuning bij de hulpverleningstaak van de politie en het leveren van een dienst of product.
5.1.2.i	Forensisch softwarebedrijf 5.1.2.i is een organisatie die software ontwikkelt voor het veiligstellen van gegevens op mobiele telefoons. De politie maakt van de diensten van 5.1.2.i gebruik op het moment dat het de digitaal rechercheur van de politie of het NFI niet lukt om gegevens op de inbeslaggenomen mobiele telefoon veilig te stellen. 5.1.2.i ontvangt politiegegevens op grond van artikel 19 Wpg.
5.1.2.i	5.1.2.i is een organisatie die tolkdiensten aanbiedt. Deze tolken zijn beëdigd. De digitaal rechercheur maakt, indien dit noodzakelijk is voor het digitaal onderzoek, gebruik van deze tolkdiensten. Bijvoorbeeld voor het vertalen van teksten of geluidsopnames. De tolk die de teksten en/of geluidsopnames vertaalt krijgt geen politiegegevens toegestuurd, maar krijgt inloggegevens om op het politiebureau de teksten en/of geluidsopnames te kunnen beluisteren en vertalen. Op grond van artikel 6 lid 4 Wpg mogen personen die niet zijn benoemd tot ambtenaar van politie, maar wel kunnen bijdragen aan de opsporing van strafbare feiten worden geautoriseerd voor het verwerken van politiegegevens voor een bepaald onderzoek. Ook in dit geval is er sprake van verstrekking in de zin van artikel 1 sub d Wpg. Het begrip verstrekken omvat iedere vorm van het bekend maken of ter beschikking stellen van politiegegevens, ongeacht de wijze waarop dit gebeurt (mondeling, schriftelijke of langs elektronische weg).[21]

16. Doorgifte aan derde landen

Beoordeel of de doorgifte van politiegegevens aan derde landen voldoet aan artikel 17a Wpg.

Naam derde landen	Toetsing doorgifte
Niet van toepassing.	Niet van toepassing.

17. Noodzakelijkheid, rechtmatigheid en doelbinding

Politiegegevens worden slechts verwerkt als dit noodzakelijk is voor de wettelijke doeleinden, behoorlijk en rechtmatig is, de gegevens rechtmatig zijn verkregen, gelet op de doeleinden toereikend, ter zake dienend en niet bovenmatig zijn, artikel 3 lid 1 en 2 Wpg.

19a. Beoordeel of de verwerking en de verdere verwerkingen zoals terbeschikkingstellingen en verstrekkingen voldoen aan de criteria van noodzakelijkheid, rechtmatigheid en doelbinding:

Criteria	Toelichting

[21] Kamerstukken II 2005/06, 30 327, nr. 3, p. 25

Proportionaliteit *Staat het belang van de verwerking in verhouding tot de beperking van de persoonlijke levenssfeer?*	Het belang van de verwerking staat in verhouding tot de beperking van de persoonlijke levenssfeer van verdachte(n) en overige betrokkenen. Het uitvoeren van digitaal onderzoek is namelijk gerechtvaardigd, omdat er een dringende maatschappelijke behoefte bestaat om het legitieme doel, zijnde opsporing en vervolging van strafbare feiten, te vervullen. Daarnaast is het uitvoeren dan digitaal onderzoek ook gerechtvaardigd, omdat het gepleegde strafbare feit in sommige gevallen alleen kan worden aangetoond door het uitlezen van elektronische gegevensdragers en/of geautomatiseerde werken. Bijvoorbeeld als het gaat om het in bezit hebben van kinderpornografie.
Subsidiariteit *Zijn andere minder in de persoonlijke levenssfeer van de burger ingrijpende maatregelen mogelijk?*	Het uitvoeren van digitaal onderzoek is een opsporingsbevoegdheid die de opsporingsambtenaar van politie ten behoeve van een opsporingsonderzoek door de digitaal rechercheur kan laten uitvoeren. Hoewel deze opsporingsbevoegdheid ingrijpend is en een groot inbreuk maakt op de persoonlijke levenssfeer van de betrokkene(n), is er geen andere minder ingrijpende maatregel mogelijk om tot hetzelfde resultaat te komen.
Niet bovenmatig *Is de verwerking niet bovenmatig en niet meer dan nodig voor het doel?*	Bij het uitvoeren van digitaal onderzoek worden meer gegevens verwerkt dan redelijkerwijs noodzakelijk is voor het doel. De gegevens die door de opsporingsambtenaar van politie worden verwerkt zijn afhankelijk van de gegevens die op het 'bestandsysteem' van de uitgelezen elektronische gegevensdragers en/of geautomatiseerde werken zijn of waren opgeslagen. In het belang van digitaal onderzoek is het onvermijdelijk en gerechtvaardigd dat er meer gegevens worden verwerkt dan noodzakelijk is. Door de gehele elektronische gegevensdragers en/of geautomatiseerde werken uit te lezen kan zowel belastende als ontlastende informatie worden verkregen en kan de opsporingsambtenaar van politie aantonen dat er geen wijzigingen zijn aangebracht in de forensische kopie. Wel worden er technische maatregelen genomen om de communicatie tussen geheimhouder(s)[22] en verdachte buiten het opspringsonderzoek te houden. Met analyseapparatuur wordt de communicatie gefilterd en verwijderd. Let wel: het verwijderen van de communicatie gebeurt alleen in de veiliggestelde gegevens die worden geanalyseerd (gegevens op de Exportmap). De forensische kopie blijft ongewijzigd.

19b. Beoordeel of de gegevens rechtmatig zijn verkregen

Rechtmatige verkrijging	Toetsing
Rechtmatigheid verkrijging	Doorzoeken ter inbeslagname is rechtmatig als de voorwerpen vatbaar zijn voor inbeslagname en de beslaglegger daartoe bevoegd is. Vatbaar voor inbeslagname zijn alle voorwerpen die kunnen dienen om de waarheid aan de dag te brengen.[23] Bijvoorbeeld elektronische gegevensdragers en/of geautomatiseerde werken waarop mogelijk sporenmateriaal te vinden is. De opsporingsambtenaar en de (hulp-)officier van justitie zijn onder bepaalde voorwaarden tot inbeslagneming bevoegd. Deze voorwaarden zijn neergelegd in de artikelen 56, 95, 96, 96a, 96b en 551 Sv ten aanzien van de opsporingsambtenaar en in de artikelen 56, 96c, 97 en 100 Sv ten aanzien van de (hulp-)officier van justitie. Overigens is de rechter-commissaris (artikelen 104, 105, 110, 195 en 114 Sv) bevoegd tot inbeslagneming.

[22] Personen die uit hoofde van hun stand, beroep of ambt tot geheimhouding verplicht zijn. Bijvoorbeeld medici, advocaten en notarissen.
[23] Art. 94 lid 1 Wetboek van Strafvordering

18. De verwerker

De politie kan een verwerker inschakelen om politiegegevens onder het gezag van de politie te verwerken (artikel 6c Wpg).

18a. Beoordeel of een externe partij een verwerker is.

Externe partij	Toetsing verwerker	Ja	Nee	Beoordeling
5.1.2.i	De dienstverlening (primaire opdracht) van de verwerker is gericht op het verwerken van politiegegevens ten behoeve van de verwerkingsverantwoordelijke	X		5.1.2.i is verwerker
	De verwerker heeft geen zeggenschap over de verwerking en handelt onder de verantwoordelijkheid van de verwerkingsverantwoordelijke en naar diens instructies. (Verwerkingsverantwoordelijke beslist over doelen van de verwerking en de middelen).	X		
	De verwerker is niet aan het rechtstreeks gezag van de verwerkingsverantwoordelijke onderworpen.	X		
5.1.2.i	De dienstverlening (primaire opdracht) van de verwerker is gericht op het verwerken van politiegegevens ten behoeve van de verwerkingsverantwoordelijke	X		5.1.2.i is verwerker
	De verwerker heeft geen zeggenschap over de verwerking en handelt onder de verantwoordelijkheid van de verwerkingsverantwoordelijke en naar diens instructies. (Verwerkingsverantwoordelijke beslist over doelen van de verwerking en de middelen).	X		
	De verwerker is niet aan het rechtstreeks gezag van de verwerkingsverantwoordelijke onderworpen.	X		

18b. Is er een verwerkersovereenkomst afgesloten?

- ☐ Ja
- ☐ Nee
- ✓ Onbekend

18c. Is de verwerkersovereenkomst volgens het format van de politie afgesloten?

- ☐ Ja
- ☐ Nee
- ✓ Onbekend

18d. Zijn de informatiebeveiligings- en Wpg eisen van de politie in de verwerkersovereenkomst opgenomen?

☐ Ja
☐ Nee
✓ Onbekend

Toelichting:

De politie maakt gebruik van webapplicatie [redacted] van [redacted] om te voldoen aan de wettelijke registerplicht en GEB-verplichting. [redacted] fungeert primair als verwerkingsregister waar alle verwerkingen met politiegegevens van de politie in moeten staan. [redacted] heeft de mogelijkheid om aan een verwerking relevante documenten te koppelen, waaronder een afgesloten verwerkersovereenkomst of uitgevoerde GEB's. In de praktijk komt het structureel voor dat van deze mogelijkheid geen gebruik wordt gemaakt. Hierdoor is het onduidelijk of verwerkersovereenkomsten zijn afgesloten en zo ja, waar deze dan zijn opgeslagen. Dit geldt ook voor de verwerkersovereenkomst met [redacted] en [redacted]. Ook hiervan is onduidelijk of deze zijn afgesloten en waar de overeenkomst is opgeslagen. De (verwerkers)overeenkomst is een juridisch dwingend instrument waarmee de politie naleving van de wet door de verwerker kan afdwingen. Als de (verwerkers)overeenkomst onvindbaar is, is het onduidelijk welke afspreken er met de verwerker zijn gemaakt en kan hier geen controle op plaatsvinden.

19. Beoordeling verwerkingstermijnen

Het gaat om de verwerkingstermijnen van artikel 8, 9, 10, 12 en 13 Wpg. Voeg aanvullende informatie toe in het tekstveld.

19a. Toets de feitelijke hantering van verwerkingstermijnen zoals genoemd in deel A aan de wettelijke termijnen.

Wettelijke politietaak Art. 8, 9, 10, 12 of 13 Wpg	Wettelijke termijn	Feitelijke termijn	Conclusie
Artikel 9 Wet politiegegevens	**Artikel 8 Wpg** Politiegegevens die op grond van artikel 8 lid 1 Wpg zijn verwerkt worden als uitgangspunt maximaal vijf jaar verwerkt. Na het verstrijken van de vijf jaar moeten de politiegegevens worden verwijderd. Verwijderde politiegegevens hebben een bewaartermijn van vijf jaar, te rekenen vanaf het moment dat deze gegevens zijn verwijderd.[24] Na het verstrijken van de bewaartermijn moeten de politiegegevens worden vernietigd, tenzij deze gegevens in aanmerking komen voor bewaring, en latere overbrenging naar het Nationaal Archief.[25]	**BVH** De politiegegevens die op grond van artikel 8 lid 1 Wpg zijn verwerkt worden in de praktijk niet vernietigd. Dit met het oog op cold case onderzoek. **Summ-IT** Summ-IT is ingericht op de bewaar- en vernietigingstermijnen van artikel 9 Wpg. De termijnen beginnen te lopen vanaf het moment dat het opsporingsonderzoek handmatig door de opsporingsambtenaar van politie op status 'voltooid' is gezet. Een dossier wordt door de ambtenaar van politie in de praktijk pas op	Er wordt niet voldaan aan de wettelijk termijnen die gelden voor het verwerken, vernietigen en bewaren van politiegegevens zoals opgenomen in de Wpg.

[24] Art. 14 lid 1 Wet politiegegevens
[25] Art. 14 lid 4 Wet politiegegevens

	Artikel 9 Wpg De verwerkingstermijn voor de politiegegevens die op grond van artikel 9 lid 1 Wet politiegegevens zijn verwerkt, is afhankelijk van de duur van het opsporingsonderzoek. Zodra het doel van het opsporingsonderzoek is behaald, vervolging niet mogelijk is of de politiegegevens niet meer noodzakelijk zijn voor het opsporingsonderzoek, worden de gegevens verwijderd of gedurende een periode van maximaal een half jaar verwerkt om te bezien of de verwerkte politiegegevens aanleiding geven voor een nieuw onderzoek.[26] Verwijderde politiegegevens hebben een bewaartermijn van vijf jaar, te rekenen vanaf het moment dat deze gegevens zijn verwijderd.[27] Na het verstrijken van de bewaartermijn moeten de politiegegevens worden vernietigd, tenzij deze gegevens in aanmerking komen voor bewaring, en latere overbrenging naar het Nationaal Archief.[28]	status 'voltooid' gezet na een afdoeningsbericht van het OM. In de praktijk komt het structureel voor dat het afdoeningsbericht van het OM achterwege blijft, met als gevolg dat dossiers zich langer in de operationele omgeving bevinden dan wettelijk is toegestaan. Als een opsporingsonderzoek wel op status 'voltooid' wordt gezet worden de politiegegevens in Summ-IT na het verstrijken van de bewaartermijn niet vernietigd. De gegevens worden achter een schot geplaats waarbij het onderzoeksdossier door het functioneel beheer weer op actief kan worden gezet.	

[26] Art. 9 lid 4 Wet politiegegevens
[27] Art. 14 lid 1 Wet politiegegevens
[28] Art. 14 lid 4 Wet politiegegevens

C. Beschrijving en beoordeling risico's en maatregelen

De privacy risicoanalyse Wpg

De privacy risicoanalyse is gebaseerd op het model DPIA-rijksdienst 2021. Het formulier maakt onderdeel uit van het format GEB-formulier Wpg maar kan ook als zelfstandig formulier worden gebruikt. Het gaat bij privacy risico's primair om de gevolgen voor de betrokkene. Naast de risico's voor de betrokkene, bestaan er ook risico's voor de organisatie. Voor de inschatting van de risico's wordt onderstaande risicomatrix, waarderingstabel toegepast. Het tweede deel bestaat uit de geadviseerde maatregelen en een inschatting van het restrisico voor en na het nemen van mitigerende maatregelen. De risico's en maatregelen zijn in overeenstemming met de Wpg bijv. met betrekking tot de doelen van de verwerking en de verwerking van bijzondere gegevens. Onder gegevens wordt verstaan politiegegevens in de zin van artikel 1 Wpg.

23. Risico´s en maatregelen

Beschrijf en beoordeel de risico's van de gegevensverwerkingen voor de rechten en vrijheden van betrokkenen. Secundair gaat het om de risico's voor de organisatie. Ga hierbij in ieder geval in op welke negatieve gevolgen de gegevensverwerkingen kunnen hebben voor:

- De rechten en vrijheden van de betrokkenen, zoals het verbod op discriminatie;
- De oorsprong van deze gevolgen;
- De waarschijnlijkheid (kans) dat deze gevolgen zullen intreden;
- De ernst (impact) van deze gevolgen voor de betrokkenen wanneer deze intreden.

Risicomatrix verwerkingen Wpg

		Impact				
		1. Verwaarloosbaar	**2. Minimaal**	**3. Gemiddeld**	**4. hoog**	**5. Kritisch**
Kans	**5. Zeer groot**	**5** GEMIDDELD	**10** GEMIDDELD	**15** HOOG	**20** KRITISCH	**25** KRITISCH
	4. Groot	**4** GEMIDDELD	**8** GEMIDDELD	**12** HOOG	**16** HOOG	**20** KRITISCH
	3. Gemiddeld	**3** LAAG	**6** GEMIDDELD	**9** GEMIDDELD	**12** HOOG	**15** HOOG
	2. Klein	**2** LAAG	**4** LAAG	**6** GEMIDDELD	**8** GEMIDDELD	**10** GEMIDDELD
	1. Zeer klein	**1** VERWAARLOS-BAAR	**2** LAAG	**3** LAAG	**4** GEMIDDELD	**5** GEMIDDELD

		Impact				
		1. Verwaarloosbaar	**2. Minimaal**	**3. Gemiddeld**	**4. hoog**	**5. Kritisch**
	Privacy	Zeer weinig impact voor de betrokkene.	Beperkte impact voor de betrokkene betreffende **algemene** persoonsgegevens.	Gemiddelde impact voor de betrokkene betreffende **algemene persoonsgegevens en/of te relateren aan een overtreding.**	Ernstige impact voor de betrokkene betreffende **algemene** persoonsgegevens en **bijzondere** persoonsgegevens of **persoonsgegevens te relateren aan een misdrijf.**	Ernstige impact voor wat betreft de rechten van betrokkenen betreffende **algemene** persoonsgegevens en **bijzondere** persoonsgegevens of persoonsgegevens te relateren aan een **ernstig misdrijf.**

14. Geconstateerde privacy risico's en maatregelen

Categorieën	Geconstateerde privacy issues/risico's	Kans	Impact	Risico Inschatting	Geadviseerde maatregelen	Kans	Impact	Restrisico
1. Organisatie								
Bewaar- en vernietigingstermijnen	**Issue**: Een onderzoeksdossier wordt door de opsporingsambtenaar van politie in de praktijk pas op afgehandeld gezet na een afdoeningsbericht van het OM. Doordat dit proces niet is geautomatiseerd en/of een afdoeningsbericht structureel achterwege blijft, komt het in de praktijk veelvuldig voor dat dossiers met daarin politiegegevens blijven staan op status "verwerken" en daardoor gegevens langer worden verwerkt dan wettelijk is toegestaan. **Risico**: Politiegegevens worden langer verwerkt dan de wettelijke termijnen waardoor er langer dan is toegestaan inbreuk wordt gemaakt op de privacy van betrokkenen. Hierdoor kan er imagoschade optreden of kan de politie een last onder bestuursdwang of bestuurlijke boete opgelegd krijgen van de Autoriteit Persoonsgegevens	**4**	**5**	**20**	Inventariseer in hoeverre wordt voldaan aan de wettelijke bewaar- en vernietigings-termijnen en pak de geconsta-teerde afwijkingen op. Maak afspraken met het OM over tijdige (bij voorkeur geautoma-tiseerde) kennisgeving met betrekking tot het sluiten van een dossier, zodat de wettelijke bewaar- en vernietigings-termijnen gaan lopen. Richt vervolgens een eigen geautoma-tiseerd proces in met betrekking tot de bewaar- en vernietigings-termijnen.	**2**	**2**	**4**

Categorieën	Geconstateerde privacy issues/risico's	Kans	Impact	Risico Inschatting	Geadviseerde maatregelen	Kans	Impact	Restrisico
	(AP) en andere onderzoeken die starten met deze gegevens een onrechtmatig basis hebben.[29]							
	Issue: Momenteel worden politiegegevens die in het politiesysteem BVH staan niet structureel vernietigd. **Risico**: Politiegegevens worden langer verwerkt dan de wettelijke termijnen waardoor er sprake is van een onrechtmatige verwerking. Als gevolg hiervan wordt er langer dan is toegestaan inbreuk gemaakt op de privacy van betrokkenen. Hierdoor kan er imagoschade optreden of kan de politie een last onder bestuursdwang of bestuurlijke boete opgelegd krijgen van de Autoriteit Persoonsgegevens (AP).	**4**	**5**	**20**	Op grond van de kamerbrief[30] worden politie-gegevens na het verstrijken van de wettelijke bewaartermijn niet vernietigd. De kamerbrief heeft waarde, maar is geen 'vrijbrief' om buiten de wet te gaan en de wettelijke bewaartermijn te overschrijden. Richt een procedure in over hoe er in de praktijk moet worden omgegaan met politie-gegevens die voor cold case onderzoek langer worden bewaard dan de termijn die op grond van de Wpg is bepaald. Bepaal welke gegevens langer dan tien jaar bewaard kunnen worden en vernietig de	**2**	**2**	**4**

[29] Art. 35c lid 1 Wet politiegegevens
[30] Kamerstuk 29628, nr. 859

Categorieën	Geconstateerde privacy issues/risico's	Kans	Impact	Risico Inschatting	Geadviseerde maatregelen	Kans	Impact	Restrisico
					overige gegevens waarvoor de bewaartermijn is verstreken.			
	Issue: Politiegegevens die in Summ-IT worden opgeslagen worden niet vernietigd. Daarnaast is er geen bewaartermijn met beperkte toegankelijkheid ingericht en zijn er geen poortwachters aangesteld. **Risico**: Politiegegevens zijn hierdoor onvoldoende beschermd en worden langer verwerkt dan de wettelijke termijnen waardoor er sprake is van een onrechtmatige verwerking. Als gevolg hiervan wordt er langer dan is toegestaan inbreuk gemaakt op de privacy van betrokkenen. Hierdoor kan er imagoschade optreden of kan de politie een last onder bestuursdwang of bestuurlijke boete opgelegd krijgen van de Autoriteit Persoonsgegevens (AP) en andere onderzoeken die starten met deze gegevens een onrechtmatig basis hebben	**4**	**5**	**20**	Vernietig politie-gegevens die in Summ-IT staan waarvan de bewaartermijn is verstreken.	**2**	**2**	**4**

Categorieën	Geconstateerde privacy issues/risico's	Kans	Impact	Risico Inschatting	Geadviseerde maatregelen	Kans	Impact	Restrisico
Verwerkingsregister	**Issue**: Afgesloten Verwerkers-overeenkomsten worden structureel niet in het daarvoor bestemde register 5.1.2.I opgeslagen. **Risico**: Het risico is dat verwerkers-overeenkomsten niet meer teruggevonden kunnen worden en het daardoor onduidelijk is of de naleving van de wet door de verwerker is afgedwongen met een juridisch dwingend instrument. Er kan hierdoor geen controle vinden op de naleving van de gemaakte afspraken.	4	3	12	Beoordeel per verwerking welke ketenpartners bij de verwerking betrokken zijn. Toets vervolgens of de ketenpartner in de zin van artikel 1 sub i Wpg een verwerker is. Zo ja, kijk of er een verwerkers-overeenkomst is afgesloten. Sluit een verwerkers-overeenkomst af indien dit niet is gebeurd. Sla de ondertekende verwerkers-overeenkomst op onder de juiste verwerking in 5.1.2.I	2	2	4
Verwerkers-overeenkomst	**Issue**: Het is onduidelijk of er verwerkers-overeenkomsten zijn gesloten met partners als 5.1.2.I en 5.1.2.I. De verwerkers-overeenkomsten zijn niet in het verwerkingsregister 5.1.2.I geüpload en het is niet duidelijk waar ze wel zijn opgeslagen. **Risico:** 5.1.2.I				Controleer of een verwerkers-overeenkomst is afgesloten. Sluit een verwerkers-overeenkomst af indien deze ontbreekt. Is er wel een verwerkers-overeenkomst, controleer of deze actueel is. Sla de verwerkers-overeenkomst			

Categorieën	Geconstateerde privacy issues/risico's	Kans	Impact	Risico Inschatting	Geadviseerde maatregelen	Kans	Impact	Restrisico
	5.1.2.I				op in 5.1.2.I			

Gegevensbeschermings effectbeoordeling (GEB) Wpg

Aanpak problematische jeugd

Gegevensbeschermingseffectbeoordeling Wet politiegegevens

Definitief

Versie 1.0

Versie datum 16 mei 2024

Versiegeschiedenis

Versie	Versie datum	Samenvatting van de aanpassing	Gemarkeerde wijzigingen
0.15	19-10-2023	Eerste versie t.b.v. interne review	-
0.2	20-11-2023	Tweede versie t.b.v. interne review	-
0.25	5-12-2023	Derde versie t.b.v. externe review	-
1.0	13-05-202	Vierde versie met laatste aanpassingen	

Distributie

Versie	Verzend datum	Naam	Afdeling / Functie

Review commentaar

Versie	Wanneer	Wie	Functie
0.15	19-10-2023	5.1.2.e	Adviseur Privacy (programma intensivering privacy)
0.2	29-11-2023	5.1.2.e	Adviseur Privacy (programma intensivering privacy)
1.0	16-05-2024	5.1.2.e	Privacy Functionaris 5.1.2.e portefeuille ZVH ondersteunend

Inhoudsopgave

Basisinformatie

Naam van de verwerking zoals aangemeld in 5.1.2.i	Aanpak problematische jeugd
Ingangsdatum van de verwerking	Bestaande verwerking
Gemandateerd verwerkingsverantwoordelijk Portefeuillehouder en ondersteunende eenheid	Martin Sitalsing ondersteund door Midden Nederland
Politieonderdeel waar de verwerking plaatsvindt	De basisteams van elke regionale eenheid.
Contactpersoon m.b.t. deze verwerking	5.1.2.e
Privacyfunctionaris	5.1.2.e

Betrokken bij deze GEB	**Naam**
Privacy adviseur programma	5.1.2.e
Reviewrol privacy adviseur programma	5.1.2.e
IB Analist programma	5.1.2.e
Privacyfunctionaris portefeuille	5.1.2.e
Adviseur portefeuillehouder	5.1.2.e
Senior business expert	-
Materiedeskundige	5.1.2.e 5.1.2.e
Materiedeskundige	5.1.2.e 5.1.2.e
Materiedeskundige 5.1.2.i	5.1.2.e 5.1.2.e

Functionaris gegevensbescherming	
Advies FG nodig: ja/nee	Nee
Datum	
Toelichting: Er is invulling gegeven aan de adviesrol van de functionaris gegevensbescherming door uitvoering van een externe review door de privacyfunctionaris van 5.1.2.e , voormalig privacyfunctionaris van 5.1.2.e .	

Gezien door verwerkingsverantwoordelijke

Naam	Martin Sitalsing
Functie	Politiechef Noord-Nederland
Datum	<invullen>
Opmerkingen<invullen>	

1. Managementsamenvatting

1.1. Hoog risico verwerking

Deze managementsamenvatting van de gegevensbeschermingseffectbeoordeling (hierna: GEB) is bedoeld voor besluitvorming door de verwerkingsverantwoordelijke. Het bevat de belangrijkste bevindingen, risico´s en maatregelen voor de onderzochte verwerking.
Op de verwerking van de portefeuille zijn een GEB en een informatiebeveiligingsanalyse uitgevoerd op grond van de Wet politiegegevens (hierna: Wpg). Als een gegevensverwerking waarschijnlijk een hoog privacy-risico oplevert voor de personen over wie de politie gegevens verwerkt, is het uitvoeren van een GEB verplicht.

De criteria voor een hoog risico verwerking zijn bepaald door de Europese toezichthouder en het beleid van de politie. Deze criteria zijn opgenomen in de 'quickscan' die wordt uitgevoerd in het systeem 5.1.2.i. Hier vindt ook de registratie van de verwerking plaats.

De verwerking is als een hoog risico verwerking aangemerkt omdat:

Deze GEB ziet op de verwerking van politiegegevens bij de aanpak van problematische jeugd. De verwerking voldoet aan de volgende criteria:

- Bij de verwerking worden gegevens van kwetsbare betrokkenen verwerkt, namelijk minderjarigen.
- Omdat de aanpak van problematische jeugd ook gepaard gaat met het regelen van gepaste zorg voor de betrokkene worden er bijzondere categorieën politiegegevens verwerkt, namelijk gegevens over de gezondheid van de betrokkene, denk bijvoorbeeld aan informatie over verslavingen of psychische problematiek.

Van de verwerking gaat dus een hoog risico uit voor de betrokkenen. Het is daarom op grond van art. 4c Wpg verplicht om een GEB uit te voeren op de verwerking.

1.2. Aanpak

Deze GEB is tot stand gekomen in overleg met de adviseurs van de portefeuille en materiedeskundigen.

Betrokken bij de uitvoering van deze GEB en de gevolgde aanpak:

Door de portefeuille Zorg & Veiligheid zijn er twee materiedeskundigen aangeleverd. Er zijn meerdere inhoudelijke gesprekken gevoerd met de materiedeskundigen inzake de verschillende thema's binnen Zorg & Veiligheid. Zo zijn er ook voor het thema problematische jeugd gesprekken gevoerd. Voorts is er voor deze GEB gebruik gemaakt van de informatie op het intranet (zie voor de specifieke documenten onderdeel 11), de processenkaarten van de bedrijfsarchitectuur, informatie van de sector informatiebeveiliging, door het Openbaar Ministerie gepubliceerde informatie en informatie van het Centrum voor Criminaliteitspreventie en Veiligheid.

De ontwikkeling van de nieuwe applicatie voor de aanpak van problematische jeugd 5.1.2.i is niet meegenomen in de bevindingen over de staat van de verwerking omdat de applicatie op het moment van schrijven nog in ontwikkeling is. Er wordt op onderdelen naar 5.1.2.i verwezen met de kanttekening dat de applicatie in ontwikkeling is en dus nog aan verandering onderhevig kan zijn.

1.3. Belangrijkste bevindingen verwerking

De GEB en de IB-analyse leiden tot risico's en maatregelen gericht op onder meer de werkprocessen, de medewerkers en de systemen. Meer gedetailleerde informatie over de uitgevoerde risico analyses is te vinden in onderdelen C en D van deze GEB.

Korte beschrijving van de belangrijkste aangetroffen privacy en IB-issues en de daarvoor te treffen maatregelen:

Er zullen kwetsbaarheden geconstateerd worden die met de invoering van die nieuwe applicatie 5.1.2.i niet langer relevant zullen zijn. De implementatie van de nieuwe applicatie 5.1.2.i zal dus in feite een aantal van de risico's mitigeren.

<u>Issue 1. Mogelijk ontbreken art. 13-protocol.</u>

Risico: Het is niet duidelijk of de Politie een art. 13-protocol hanteert ten aanzien van AOLs en AOPs. Dit kan leiden tot overmatige gegevensverwerking.

Maatregel: Stel een art. 13-protocol op om de verwerking in te kaderen.

<u>Issue 2. Actualisatie registraties van jeugdgroepen in 5.1.2.i .</u>

Risico: De registraties van jeugdgroepen worden niet tijdig opgeschoond, dat betekent dat er registraties opgeslagen zijn van groepen die niet langer actief zijn of waarvan de leden allemaal meerderjarig zijn. Dit leidt tot overschrijding van de verwerkingstermijn in art. 8 Wpg.
Maatregel: Optimaal: laat verwijdering geautomatiseerd plaatsvinden. Suboptimaal: schoon periodiek 5.1.2.i de registraties op.

Issue 3. Vernietigingsbeleid 5.1.2.i

Risico: De uit 5.1.2.i verwijderde registraties komen in een archief dat niet wordt vernietigd. Dit betekent dat ook niet wordt voldaan aan de verwerkingstermijn van art. 14 Wpg. Dit beleid is conform het besluit van de korpschef dat door de Minister van Justitie en Veiligheid is bevestigd in zijn brief aan de Tweede Kamer van 4 februari 2019.[1]
Maatregel: Optimaal: laat vernietiging geautomatiseerd plaatsvinden. Suboptimaal: schoon periodiek handmatig de registraties op.

Issue 4. Autorisaties in 5.1.2.i

Risico: De autorisaties voor 5.1.2.i verlopen niet via 5.1.2.i maar via 5.1.2.i waaruit volgt dat 5.1.2.i
Maatregel: Optimaal: laat autorisatie tot de applicatie, of de opvolger 5.1.2.i, via 5.1.2.i plaatsvinden op basis van rollen. Suboptimaal: her-beoordeel periodiek alle autorisaties.

Issue 5. Audittrails 5.1.2.i.

Risico: 5.1.2.i bevat geen geschikte functionaliteit ten aanzien van het bijhouden van wijzigingen in registraties en toegang tot gegevens. (logging).
Maatregel: Gelet op de voorgenomen overstap van 5.1.2.i naar 5.1.2.i moet deze functionaliteit worden opgenomen in 5.1.2.i

Issue 6. Gebruik 5.1.2.i

Risico: In gevallen wordt 5.1.2.i gebruikt in plaats van 5.1.2.i-applicatie bij de monitoring van betrokkenen. Omdat 5.1.2.i, in tegenstelling tot 5.1.2.i, geen registratieapplicatie is wordt over een individu verwerkte informatie niet geautomatiseerd toegevoegd aan 5.1.2.i. Dat betekent dat eventuele aanvullende informatie verkregen uit 5.1.2.i handmatig aan 5.1.2.i toegevoegd moet worden. Dit kan leiden tot onvolledige gegevensverwerking ten aanzien van de met 5.1.2.i verwerkte gegevens.
Maatregel: Leidt medewerkers op in het correct gebruik van de aangewezen applicatie, 5.1.2.i of 5.1.2.i.

Issue 7. Verstrekking op grond van art. 19 Wpg

Risico: Incidentele verstrekkingen op basis van art. 19 Wpg zonder spoedeisend belang voldoen niet aan de wettelijke vereisten die volgen uit de Awb. De betrokkene wordt de gelegenheid ontzegd om zijn zienswijze te geven op de voorgenomen verstrekking. Dit leidt tot een onrechtmatige verstrekking.
Maatregel: Geef de betrokkene de gelegenheid om een zienswijze naar voren te brengen of gebruik art. 19 uitsluitend als verstrekkingsgrond in spoedeisende gevallen.

Issue 8. Gebruik 5.1.2.i

Risico: 5.1.2.i
Maatregel: 5.1.2.i

Issue 9. Beoordeling verstrekking door politieambtenaar

Risico: Verstrekkingen aan structurele en incidentele samenwerkingsverbanden worden niet conform een landelijk geldend kader uitgevoerd. Er wordt steeds door de verstrekkende politieambtenaar een individuele afweging gemaakt of verstrekking noodzakelijk is. Dit kan leiden tot verschillende verstrekkingsregimes tussen regio's.
Maatregel: Stel een landelijk kader op voor de verstrekkingen aan de samenwerkingsverbanden

1.4. Vervolgproces

Het vervolgproces voor de portefeuillehouder ten aanzien van de maatregelen:

Het is de verantwoordelijkheid van de portefeuille Zorg & Veiligheid om de risico's benoemd in deze GEB te mitigeren of te accepteren.

Mitigatie: de portefeuille komt met een plan van aanpak en implementeert maatregelen om de benoemde risico's te mitigeren.

[1] Brief van de Minister van Justitie en Veiligheid van 4 februari 2019 (*Kamerstukken II* 2018/19, 29628, nr. 859).

Acceptatie: de portefeuille besluit formeel tot het accepteren van één of meerdere risico's en beargumenteert dit. De portefeuille stelt de functionarissen gegevensbescherming in kennis van de geaccepteerde risico's en de daaraan ten grondslag liggende overwegingen.

NB: In het geval dat de portefeuille kiest voor de mitigatie van de risico's die uit het gebruik van [redacted] volgen, ligt het voor de hand om de maatregelen mee te nemen in het traject naar de nieuwe applicatie: [redacted]

A. Beschrijving kenmerken gegevensverwerking

1. Beschrijving verwerking

1a. Korte beschrijving van de context van de verwerking

De plaats in de organisatie waar de verwerking plaatsvindt en de beleidsdoelstellingen van de verwerking.

Binnen de portefeuille Zorg & Veiligheid bestaan drie hoofdthema's: problematische jeugd, personen met verward gedrag en huiselijk geweld en kindermishandeling.

Hoewel de doelgroep en doelstelling binnen deze thema's afwijkt, wordt er wel gebruik gemaakt van één aanpak die bestaat uit de volgende elementen:

- Acuut optreden bij situaties van onveiligheid;
- Signaleren, adresseren & adviseren;
- Het zijn van een betrouwbare partner voor ketenpartners.

Voor elk thema wordt een GEB opgeleverd. De GEBs kunnen raakvlakken hebben, we adviseren daarom om de GEBs in onderlinge samenhang te bekijken.

Deze GEB gaat over het verwerken van politiegegevens bij de aanpak van problematische jeugd. Elke regionale eenheid heeft in meer of mindere mate te maken met problematische jeugd(groepen). De basisteams binnen de eenheden beschikken over Zorg & Veiligheid-specialisten die onder andere voor de aanpak van problematische jeugd verantwoordelijk zijn. De verwerking vindt plaats op het niveau van de basisteams (hierna: BT) binnen de regio's.

Een belangrijk aspect in de aanpak van problematische jeugd is de samenwerking met ketenpartners en de plaats die de Politie daar inneemt.

De relevante ketenpartners zijn:

- Burgmeester (als gezagsdrager)
- de lokale gemeente (als procesregisseur)
- het OM
- zorginstellingen (diverse per district / regio)
- Veilig Thuis
- Reclassering

De regie op de aanpak van problematische jeugd ligt bij de burgemeester, specifiek een regisseur die namens de burgemeester de ketenpartners bijeenroept op basis van expertise. Dit betekent dat de Politie slechts een onderdeel vormt van de totale aanpak van problematische jeugdgroepen. De Politie wordt alleen in die gevallen betrokken waar er ook een veiligheidscomponent aanwezig is in de aanpak van een problematische jeugdgroep.

1b. De verwerking op hoofdlijnen

Hier volgt een beschrijving van de verwerking van begin tot eind.

Opzet

Het Centrum voor Criminaliteitspreventie en Veiligheid heeft de aanpak van problematische jeugd in een 7-stappenplan beschreven.[2] De eerste drie stappen van het 7-stappenplan bestaan uit het in kaart brengen van de case, in stap vier en vijf wordt besloten tot het volgen van een bepaalde aanpak en stap zes bestaat uit de uitvoering en monitoring van de aanpak. In stap zeven wordt de aanpak geëvalueerd en beëindigd.[3]

Scope en begrippen

In deze GEB ligt de focus op de verwerking van politiegegevens bij de aanpak van jeugd die problematisch groepsgedrag vertoont waar een verstoring van de openbare orde van uit gaat. Problematische jeugdgroepen zijn jeugdgroepen, bestaande uit twee of meer personen van maximaal 23 jaar oud, die overlast veroorzaken en als

[2] Centrum voor Criminaliteitspreventie en Veiligheid, juni 2023, *Werkproces aanpak problematische jeugdgroepen en groepsgedrag: Het 7-stappenmodel*.
[3] Centrum voor Criminaliteitspreventie en Veiligheid, juni 2023, *Werkproces aanpak problematische jeugdgroepen en groepsgedrag: Het 7-stappenmodel*, pag. 8.

zodoende een risico zijn voor de openbare orde. Denk hierbij aan hangjongeren. Wanneer problematisch groepsgedrag uitsluitend crimineel van aard is, komt de focus meer op opsporing te liggen. De aanpak van jeugdgroepen die uitsluitend voor opsporing in aanmerking komen, valt buiten de scope van deze GEB. Z&V-specialisten worden dan wel betrokken in de aanpak van criminele jeugdgroepen echter ziet dit uitsluitend op het aanjagen van opsporing en het ondersteunen in te maken keuzes in de opsporing van criminele jeugdgroepen.

De gegevensverwerking vindt voor een groot deel plaats via 5.1.2.i , 5.1.2.i wordt binnenkort vervangen door de applicatie 5.1.2.i . 5.1.2.i is een high-risk applicatie zoals vastgesteld door de Gegevensautoriteit in 2018.[4] Omdat de operatie op het moment van schrijven nog gebruik maakt van 5.1.2.i en 5.1.2.i nog niet formeel gebruikt wordt vormt 5.1.2.i geen onderdeel van de GEB. De portefeuilles Zorg & Veiligheid en PVR hebben de referentie GEB OPP RAPP ook van toepassing verklaard op de applicatie 5.1.2.i

Bij de aanpak van problematische jeugdgroepen wordt over het algemeen gebruik gemaakt van ketenpartners en overlegstructuren. De eventuele verstrekking van politiegegevens aan deze ketenpartners (al dan niet in overlegstructuren) is in scope, de werking van de verschillende overlegstructuren of de werkzaamheden van de ketenpartners is buiten scope. De overlegstructuren worden wel beschreven als dat nodig is om context te geven aan de verwerking, zonder dat deze inhoudelijk beoordeeld zullen worden.

Een groepsaanpak bestaat doorgaans uit twee niveaus, het groepsniveau en het individuele niveau. Op individueel niveau kan parallel aan de groepsaanpak een persoonsgebonden aanpak (hierna: PGA) opgestart worden. Zowel de aanpak op groepsniveau als de aanpak op individueel niveau zijn onderdeel van deze GEB.

Proces aanpak problematische jeugd
De belangrijkste ketenpartners van de politie bij de aanpak problematische jeugd zijn de burgemeester en het OM. Met hen vormt de politie de lokale driehoek. De aanpak bestaat uit een aantal onderdelen, die hierna worden beschreven. Daarbij wordt aangegeven wat de rol van de politie is in de gezamenlijke aanpak van problematische jeugdgroepen en waar in het proces politiegegevens worden verwerkt.

Begin van de verwerking (stap 1: signalen over groepsgedrag delen)
Bij de Politie begint de verwerking met het analyseren van de mutaties in BVH. De Z&V-specialist, jeugdagent, of wijkagent van een BT voert dagelijks een query uit via BlueSpot Monitor. Hieruit ontstaat een totaalbeeld van de bestaande overlast of problematiek die door een jeugdgroep veroorzaakt wordt. Er wordt op twee manieren een zoekslag gedaan, de snelle en de uitgebreide zoekslag. De snelle zoekslag geeft een overzicht van de E35-mutaties (E35: Melding overlast jeugd) binnen een bepaald geografisch gebied in een datumbereik.[5] De uitgebreide zoekslag is gericht op alle incidenten binnen een geografisch gebied in een datumbereik waarvan de betrokkenen jonger dan 23 jaar oud zijn Er is geen landelijk beleid over het uitvoeren van de uitgebreide zoekslag naar overlast door problematische jeugd of de parameters die daarbij gebruikt moeten worden. Dit wordt binnen de verschillende regio's op eigen inzicht door de Z&V-specialist uitgevoerd.

Bespreking jongerentafel (vervolg stap 1: signalen over groepsgedrag delen; stap 2: beoordelen groepsgedrag)
De gesignaleerde overlastlocaties worden besproken in een jongerentafeloverleg, waarin enkel locatie en de aard van de incidenten ter sprake komt en niet de individuen waar een groep uit bestaat, waarna de casusregisseur van de gemeente opdracht geeft aan de Politie tot het doen van een groepsscan. De jongerentafel is een overleg waarin de gemeente (met vertegenwoordigers van handhaving en jongerenwerk), de wijkmanager en de wijkagent overleg hebben. De verantwoordelijkheid voor de regie op de aanpak van jeugdgroepen ligt bij de gemeente. Gelet op de aard van de problematiek (overlast & openbare veiligheid) is de burgemeester gezagsdrager.

Groepsscan (stap 3: groepsduiding en concept pva opstellen)
Een groepsscan houdt in dat de individuen waaruit de groep bestaat geïdentificeerd worden en gekoppeld worden aan de (eventuele) strafbare feiten (en andere art. 8 informatie) waar de groep zich van bedient.

Een individu wordt door de Politie als onderdeel van een groep beschouwd als deze bij een ID-controle is voorgekomen in samenhang met andere jongeren. In de praktijk betekent dit dat er op een bekende overlastlocatie een ID-controle wordt gehouden waarbij alle aanwezige jongeren, ongeacht hun gedragingen, als groepslid worden gekwalificeerd.

De resultaten van de groepsscan worden vervolgens gedeeld met de lokale driehoek in een rapport met leeftijdscategorieën, woonplaatsen, en soorten delicten. In het tot stand komen van het rapport worden politiegegevens verwerkt. De gegevens in het rapport zijn dit echter niet. Er worden in het overleg met de driehoek uiteindelijk wel namen gedeeld waarbij de delicten niet aangeduid worden. Ook wordt er mondeling context gegeven aan de rol die een individu heeft binnen een jeugdgroep.

[4] Zie brief van 10 april 2018, *Vaststellen highrisk applicaties tbv Privacy & Security by Design (PSbD) compliancy*, van de Gegevensautoriteit. (intranet)
[5] Een E-35 mutatie bevat één algemeen veld waarin de bevindingen en constateringen genoteerd zijn door de politieambtenaar op straat.

Tot voor kort werd gebruik gemaakt van een risicotaxatie-instrument genaamd 5.1.2.i bij het opstellen van het rapport van de groepsscan. De resultaten werden geanonimiseerd opgenomen in het rapport van de groepsscan, er werd weergegeven wat het aantal groepsdeelnemers was met een verhoogde score uit het 5.1.2.i risicotaxatie-instrument. De portefeuille Zorg & Veiligheid heeft onlangs besloten tot het staken van het gebruik van 5.1.2.i binnen de Z&V-processen. Gezien de korte tijd dat dit besluit van kracht is verdient het aanbeveling om na te gaan welke impact het besluit heeft op de operationele processen (zoals het uitvoeren van de groepsscan).

5.1.2.i wordt zowel gebruikt voor het aanduiden van de groep als voor het uitvoeren van de groepsscan. In de praktijk werken collega's minder in 5.1.2.i vanwege gebruiksonvriendelijkheid. Dit heeft tot gevolg dat 5.1.2.i gebruikt wordt voor het monitoren van individuen door middel van abonnementen. 5.1.2.i is een registratie-applicatie waarvan de gegevens geautomatiseerd toegevoegd worden aan de 5.1.2.i . 5.1.2.i is dit niet. Eventuele aandachtsvestigingen of aanvullende informatie op een individu moet bij gebruik van 5.1.2.i handmatig worden toegevoegd in BVH anders wordt het voor andere politieambtenaren niet duidelijk dat een individu in scope is voor een (begin van een) aanpak problematische jeugd. Dit werkt 'losse eindjes' in de hand waar het gaat om registratie van informatie. Zo gaat bijvoorbeeld het beëindigen van een abonnement in 5.1.2.i niet automatisch gepaard met het aanpassen van informatie in de persoonskaart van een individu die eerst wél maar inmiddels niet langer in scope voor een aanpak is. Zo kan een individu abusievelijk langer aangeduid worden als lid van een jeugdgroep dan noodzakelijk is.

In tegenstelling tot 5.1.2.i wordt in 5.1.2.i gewijzigde informatie wel geautomatiseerd opgenomen in de informatie die de politieambtenaar op straat te zien krijgt.

PGA
Naar aanleiding van de vergaarde informatie kan de Z&V-specialist personen uit de groep aanmerken als zijnde 'geprioriteerde politiepersonen'[6] indien de door hen gepleegde delicten binnen de lokaal geselecteerde veiligheidsthema's vallen. Deze personen worden door de specialist op een politienamenlijst geplaatst. Vervolgens wordt er door middel van 5.1.2.i informatie opgehaald over de gepleegde delicten en Preselect Recidive score.[7] Deze lijst wordt vervolgens opgeschoond, de personen voor wie reeds een PGA loopt worden niet opnieuw meegenomen, eveneens personen die gedetineerd zijn of jegens wie een opsporingsonderzoek loopt worden niet meegenomen. De overgebleven namen worden doorgegeven aan de relevante basisteams in een Excel-bestand per mail.[8] Ook wordt de lijst door de 5.1.2.i bewaard. Op de geprioriteerde politiepersonen kan een PGA worden opgestart. Dit vindt onafhankelijk van de groepsaanpak plaats maar vormt wel een factor die betrokken wordt in de aanpak van een groep.

Het is onduidelijk welke impact het eerdergenoemde besluit ten aanzien van het staken van het gebruik van 5.1.2.i binnen de portefeuille Z&V zal hebben op het PGA-proces.

Vervolgaanpak (vervolg stap 3: groepsscan en plan van aanpak opstellen; stap 4: Adviseren en prioriteren; stap 5: vaststellen plan van aanpak)
Na het jongerentafeloverleg en de groepsscan kan een verdere behandeling van een problematische jeugdgroep op de volgende drie manieren vorm krijgen:

- Bespreking met de lokale driehoek, deze bestaat uit de burgemeester, Politie, en het Openbaar Ministerie.
- Bespreking in een incidenteel overleg, hierbij worden de ketenpartners door de gemeente naar aard van de casus bijeengebracht.
- Bespreking in een regionaal Zorg- en Veiligheidshuis, dit geldt uitsluitend voor de bijzonder complexe gevallen. Deze bestaat structureel uit: Gemeenten, OM, politie, 3RO, RvdK, (jeugd)zorg, ggz, gehandicaptenzorg, DJI. Incidenteel kunnen er aanvullende ketenpartners bij betrokken worden, denk hierbij aan UWV, maatschappelijk werk, of woningcorporaties.

De bespreking van de casus in een van de drie overlegvormen gaat gepaard met de verstrekking van politiegegevens aan de in het overleg deelnemende ketenpartners. De verstrekkingen worden geanalyseerd in dit document, de verwerking van gegevens binnen de verschillende overlegvormen echter niet omdat dit geen verwerking van politiegegevens betreft.

In deze fase wordt door de procesregisseur vanuit de gemeente geadviseerd over de aanpak van de groep en de prioritering.

In de behandeling van de casus met de drie verschillende soorten gremia komt steeds een gezamenlijk plan van aanpak tot stand. De casus worden steeds met tussenpozen besproken waarbij doorlopend zowel de effectiviteit

[6] Een geprioriteerd politiepersoon is iemand die enerzijds strafbare feiten, die landelijk of lokaal geprioriteerd zijn, heeft gepleegd, of van wie verwacht wordt dat hij/zij deze zal plegen en die anderzijds volgens de politie in aanmerking komt voor een Persoonsgerichte Aanpak vanuit het bevoegd gezag. Zie webapp PGA: link.
[7] Zie de instructie voor het gebruik van 5.1.2.i op het intranet.
[8] Gebaseerd op het werkveld van het basisteam en de woon- of verblijfplaats van de betrokkene.

en de noodzaak van de aanpak besproken wordt. Dit betekent dat de aanpak aangepast of gestaakt kan worden door veranderende omstandigheden.

Verwerking van politiegegevens in de groeps- of persoonsgerichte aanpak (stap 6: Uitvoeren en monitoren plan van aanpak)
Een groeps- of persoonsgerichte aanpak krijgt bij de Politie praktisch vorm in aandachtsvestigingen, afspraken op locatie of andere toevoegingen in de persoonskaart van een individu in de BVH. Aantekeningen op groepsniveau worden bij elk groepslid toegevoegd, individuele aantekeningen uitsluitend aan de kaart van het betreffende groepslid. Deze aanvullingen zijn voor de agent op straat zichtbaar zodra zij op een melding afgestuurd worden of een aangetroffen persoon op identiteit controleren. Zo kunnen de politieambtenaren op straat conform de afspraken met de ketenpartners handelen.

Einde van de groepsaanpak (stap 7: afschalen en evalueren)
De aanpak staakt zodra dit door de ketenpartners besloten wordt of alle individuen in de groep de leeftijd van 23 jaar hebben gepasseerd.

Na de beëindiging van de aanpak wordt de informatie handmatig uit 5.1.2.I verwijderd.

De verwerking eindigt op dit moment niet omdat er geen vernietiging plaatsvindt van de gegevens. Deze worden in een archief opgeslagen zonder vernietiging.

2. Big data
Er is geen sprake van een 'big data'-verwerking.

3. Motivatie hoog risico verwerking

Bij de verwerking worden gegevens van kwetsbare betrokkenen verwerkt, namelijk minderjarigen. Omdat de aanpak van problematische jeugd ook gepaard gaat met het regelen van een gepaste aanpak voor de betrokkene kunnen er bijzondere categorieën politiegegevens verwerkt worden, namelijk gegevens over de gezondheid van de betrokkene (verslavingen, psychische problematiek). In gevallen wordt deze informatie binnen 5.1.2.I opgeslagen onder de noemers keteninformatie, handelingskader, of bijzonderheden.

4. Politiegegevens
Per categorie betrokkene de politiegegevens die worden verwerkt.

4a. Beschrijving van de betrokkenen en de politiegegevens

Categorie betrokkene	Gegevens
Categorie betrokkene	**Categorie algemene politiegegevens**
Subject mutaties binnen zoekslag BVH	Naam, adres, leeftijd, BSN, delict(en), mutaties (E-35 formulier).
Lid problematische jeugdgroep, waaronder PGA-ers.	Naam, adres, woonplaats, postcode, BSN, delict(en), mutaties gerelateerd aan gedrag in problematische jeugdgroep (E-35 mutaties), handelingskader vastgesteld in samenspraak met ketenpartners.
Verbalisant registraties BVH	Naam, dienstnummer.
Categorie betrokkene	**Categorie bijzondere politiegegevens**
Lid problematische jeugdgroep binnen groepsaanpak	Gezondheidsinformatie (in de aanvullingen / het handelingskader op de persoonskaart)

4b. De omvang van de gegevensverwerking op jaarbasis en landelijk gezien

Omvang	Antwoord
Aantal betrokkenen die in de verwerking voorkomen, indien mogelijk per systeem	Er ontbreken recente landelijke cijfers. Er zijn landelijk 40.000 individuen in 5.1.2.I aangemerkt, deze applicatie wordt gebruikt voor meerdere doelgroepen, het is onduidelijk hoeveel registraties er binnen de jeugddoelgroep zijn.
Reikwijdte verwerking	Regionaal.

Duur van de verwerking	Afhankelijk van de gevolgde aanpak, als het volledige proces uitgelopen wordt, duurt de verwerking totdat de overlegtafel die tot de aanpak besloten heeft, besluit dat de aanpak niet langer opportuun is óf dat alle leden van de groep de leeftijd van 23 bereikt hebben. De individueel toegevoegde aandachtsvestigingen in BVH verlopen na maximaal vijf jaren. Er kan een kortere geldigheidsduur worden ingesteld bij het opstellen van de aandachtsvestiging, deze heeft echter geen invloed op de verwerkingstermijn. De informatie die in 5.1.2.I is toegevoegd (keteninformatie, individuele en groepsinformatie) wordt niet meer aan de BVH (en dus de 5.1.2.I) geleverd op het moment dat de registratie gearchiveerd wordt. Voor wat betreft de PGA, deze aanpak kan de aanpak problematische jeugdgroepen qua duur overstijgen. De duur is afhankelijk van de gevolgde aanpak, deze kan periodiek beoordeeld worden of eenmalig voor een bepaalde duur vastgesteld worden.
Frequentie van de verwerking	De frequentie van de verwerking is afhankelijk van de situatie op straat en het bestaan van problematische jeugd of jeugdgroepen. Er is dus geen vaste frequentie waarop deze verwerking plaats vindt.

4c. Dataoverzichten per applicatie

4c.1. Data overzicht naam applicatie: 5.1.2.I

5.1.2.I

Toelichting:

5.1.2.I voegt informatie toe aan BVH-registraties, deze informatie wordt vervolgens doorgezet naar de 5.1.2.I . De 5.1.2.I kan vervolgens door middel van 5.1.2.I , 5.1.2.I , en MEOS bevraagd worden. De 5.1.2.I , 5.1.2.I , (en 5.1.2.I)[9] zijn/waren varianten 5.1.2.I -rapportages.

4c.2 Data overzicht naam applicatie: 5.1.2.I 5.1.2.I

[9] Inmiddels niet meer in gebruik conform beleid portefeuille Zorg & Veiligheid.
[10] De beschikbare info hierover op intranet, zie: Beschrijving functionaliteit 5.1.2.I , 2015. (intranet: link)

Toelichting:

vraagt informatie op uit , welke wordt aangevuld vanuit de registratieapplicaties.

4c.3 Data overzicht naam applicatie:

Toelichting:

vraagt informatie op uit , welke wordt aangevuld vanuit de registratieapplicaties. Zie voor het dataoverzicht.

5. Gegevensstroom

Onderstaand de gegevensstroom aan de hand van de verschillende stadia van de verwerking. De middelen en systemen die voor de verwerking gebruikt worden zijn ook beschreven.

5a. De stadia van de gegevensstroom

Stadia verwerking	Beschrijf de handelingen van de verwerking	Middelen, landelijke systemen, EBO's
Start van de verwerking, herkomst van de gegevens, wijze van verkrijging	De dagelijkse zoekslag van de Z&V-taakaccenthouder op overlast en dergelijke vindt plaats via . Deze applicatie zoekt in de mutaties in BVH via .	BVH,
Vastleggen, ordenen, structureren, bijwerken of wijzigen, gebruiken, raadplegen, combineren, afschermen	Vervolgens worden de politiegegevens van individuen bij de selectie van geprioriteerde politiepersonen en groepsleden uit BVH gelezen. De gegevens van geprioriteerde politiepersonen of aangemerkte groepsleden worden vervolgens in geplaatst. Hier worden de personen gegroepeerd. Na opdracht van de gemeente wordt er een groepsscan gedaan op de vastgestelde groep.	BVH
Resultaten, producten van de verwerking	Groepsrapport naar aanleiding van de groepsscan van de problematische jeugdgroep. De politienamenlijst met namen van geprioriteerde politiepersonen wordt opgesteld op basis van de eerder opgehaalde informatie over gepleegde delicten en bestaande problematiek. Informatie over de aanpak wordt toegevoegd op groeps- en individueel niveau. Dit betreft het door de Politie in samenspraak met ketenpartners opgestelde handelingskader.	Rapport groepsscan: Politienamenlijst: Informatie over aanpak: BVH,
Verwijderen van gegevens (meer gedetailleerd in vraag 10)	Na einde van de aanpak van de jeugdgroep wordt de jeugdgroep uit verwijderd.	

	Na einde van een PGA-aanpak verlopen de aandachtsvestigingen in BVH en het daarin verwerkte handelingskader. Verwijdering uit 5.1.2.i vindt handmatig plaats. De gegevens worden dan gearchiveerd en zijn niet meer via 5.1.2.i te benaderen.	
Uitwijkvoorziening in geval continuïteit	-	-
Het verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen (meer gedetailleerd in vraag 5)	Er worden gegevens verstrekt aan de ketenpartners via de relevante overlegstructuren. Er is geen vaste Politie-applicatie voor het verstrekken van informatie aan ketenpartners buiten de zorg en veiligheidshuizen.	De zorg- en veiligheidshuizen gebruiken landelijk applicaties: 5.1.2.i, en 5.1.2.i voor de uitwisseling van informatie. Er zijn geen vaste applicaties voor de andere ketenoverleggen. Verstrekking vinden daar meestal mondeling plaats. In het geval dat er wel schriftelijk verstrekt wordt aan een ketenpartner buiten het zorg- en veiligheidshuis vindt dit per mail plaats via 5.1.2.i.
Vernietigen	Er is geen vernietigingsbeleid voor het 5.1.2.i archief. Ook na de overgang van 5.1.2.i naar 5.1.2.i wordt de database van 5.1.2.i niet vernietigd. Zie daarvoor het “Advies uitfaseren 5.1.2.i” opgesteld door DIV in samenwerking met de IV-expert van de portefeuille Z&V.	5.1.2.i

5b. BRM Werkprocessen

De volgende werkprocessen uit het bedrijfsreferentiemodel (hierna: BRM) hebben betrekking op de verwerking.

Te koppelen werkprocessen:	
534	**Bewerken lokale politie namenlijst PGA**
535	**Monitoren PGA**
536	**Monitoren probleem**
541	**Sturen op aanpak casus**
542	**Aanvragen groepsscan**
544	**Behandelen zaak door JCO-jeugd**
546	**Kiezen & routeren PGA'ers**
549	**Sturen op aanpak problematische groep**
550	**Uitvoeren preselectie Jeugd**
552	**Intake en selecteren zaken veiligheidshuis**
553	**Opstellen politienamenlijst**
554	**Selecteren personen met hoog risico**
556	**Voeren casusoverleg complexe multi probleem zaken**
557	**Voeren casusoverleg veeleisende zaken**
559	**Voorbereiden en opvolgen casusoverleg**
560	**Vormgeven aanpak veiligheidsprobleem**
561	**Vroegsignaleren probleem**

Proces 544, 550, en 561 sluiten niet goed aan op de praktijk. Proces 544 heeft betrekking op het verkorten van wachttijd voor straf of hulpverlening aan jeugdigen, 550 vindt niet langer plaats, en 561 is niet relevant voor de aanpak van jeugdgroepen.

5c. Overzicht van de gegevensstroom bijgevoegd:
Dit is beschreven in onderdeel 5a.
5d. Eigen beheerde omgeving
Als er gebruik gemaakt wordt van lokale 'eigen beheerde omgevingen' (EBO's) worden deze hieronder beschreven:

Naam EBO	Doel van de EBO	Eenheid die een EBO beheert	Eigenaar
-	-	-	-

6. Doel van de verwerking

Het doel van de (voorgenomen) gegevensverwerking en eventuele andere doelen die gerelateerd zijn aan de verwerking. Beschrijving van het concrete doel en de richting van de verwerking.

Verwerking	Doel van de verwerking
Aanpak problematische jeugdgroepen	Het bestrijden en voorkomen van overlast door problematische jeugd en het meewerken aan het verzorgen van de juiste zorg voor problematische jeugd op individueel en groepsniveau.

7. Betrokken partijen en hun belangen

Benoem welke partijen binnen het politiedomein en buiten het politiedomein (externe partijen) betrokken zijn bij de (voorgenomen) gegevensverwerking. Het gaat om hun rol en belang als ontvanger, verstrekker of verwerker. Beschrijf de politiegegevens die aan deze partijen worden verstrekt. Voor de indeling van de externe partijen is gebruik gemaakt van paragraaf 3 van de Wpg.

Partij	Rol en belang partijen	Politiegegevens
Binnen het politiedomein	Taakaccenthouder Z&V, ontvanger en verstrekker	Naam, adres, leeftijd, BSN, delict(en), mutaties (E-35 formulier), handelingskaderinformatie in BVH en 5.1.2.I .
	Wijkagent, ontvanger en verstrekker	Naam, adres, leeftijd, BSN, delict(en), mutaties (E-35 formulier), handelingskaderinformatie in BVH en 5.1.2.I
	Basisteam, ontvanger.	Naam, adres, leeftijd, BSN, delict(en), mutaties (E-35 formulier) handelingskader in BVH.
	OSB Z&V, ontvanger en verstrekker.	Naam, adres, leeftijd, BSN, delict(en), mutaties (E-35 formulier), handelingskaderinformatie in BVH en 5.1.2.I .
Externe partijen		
Gezagsdrager:	Burgemeester, ontvanger.	Bij bespreking in de driehoek: Namenlijst van de groepsleden; gepleegde delicten / overlastbeeld.
Derde incidenteel:	Gemeente, zorgpartijen, woningcorporaties, reclassering. Ontvangers.	Bij incidenteel overleg op groepsniveau: Namenlijst van de groepsleden; gepleegde delicten / overlastbeeld. Incidenteel bij een persoonsgerichte aanpak: Personalia / BSN; gepleegde delicten en bekende problematiek.
Derde structureel samenwerkingsverband:	Regionaal jongerentafeloverleg, lokale driehoek, regionaal	De lijst met namen van de jeugdgroep, inclusief een overzicht

	veiligheidshuis. Ontvangers.	van de gepleegde delicten. Deze informatie is niet aan elkaar gekoppeld. In gevallen kan er op individueel niveau tot een PGA besloten worden. Dan wordt de identiteit van de betrokkene onderling vastgesteld door middel van een BSN. Ook worden er gegevens gedeeld over de relevante interacties met de Politie. De informatie wordt vooraf op relevantie beoordeeld door de verstrekkende ambtenaar, deze maakt per overleg een I90-formulier op om de verstrekking te administreren en te motiveren.

8. Autorisaties

Politiegegevens worden slechts verwerkt door ambtenaren van de politie die daartoe door de verwerkingsverantwoordelijke zijn geautoriseerd en voor zover de autorisatie strekt.

Licht toe hoe het autorisatiebeheer concreet voor deze verwerking functioneert

Meerdere antwoorden zijn mogelijk zo nodig per systeem beschrijven

Inrichting autorisaties	Ja	Nee	Nadere toelichting
5.1.2.I			

9. Verwerkingslocaties

Onderstaand wordt beschreven in welke landen de verwerking plaatsvindt. In het geval van een doorgifte aan een derde land of internationale organisatie wordt dit apart benoemd.

De verwerking vindt plaats in:

Nederland

10. Verwerkingstermijnen

In dit onderdeel wordt beschreven hoe de verwerkingstermijnen in de praktijk worden gehanteerd. Het gaat om de feitelijke hantering van de verwerkingstermijnen. Ook hoe de gegevens verwijderd, vernietigd en gearchiveerd worden is relevant evenals welke individuen deze handelingen uitvoeren.

Antwoord:

De in 5.1.2.I aangemaakte groepen en toegevoegde personen moeten handmatig verwijderd worden. Dit gebeurt niet consistent. Dit betekent dat de situatie soms ontstaat dat er jeugdgroepen geregistreerd staan waarvan de leden niet langer in de doelgroep van aanpak problematische jeugd (tot 23 jaar oud) vallen.

Daarbij komen in [redacted] verwijderde records in het archief van [redacted]. Er is geen vernietigingsbeleid van toepassing op het [redacted] archief. Deze worden ook na de overgang op [redacted] vanaf 1 januari 2024 nog vijf jaren doorzoekbaar waarna ze afgeschermd zullen worden.

11. Juridisch en beleidsmatig kader

Wetgeving en beleid speelt een rol voor de gegevensverwerking. De relevante artikelen en beleidsstukken worden hieronder weergegeven. De Wpg wordt elders in dit document al afdoende beschreven en dus buiten dit onderdeel gehouden.

Juridisch en/of beleidsmatigkader	Wetsartikelen
Eén aanpak Zorg en Veiligheid, Jeugdplan 2021	
Zorg & Veiligheid, Jaarplan en realisatieplan: Denken én Doen in 2021	
Werkproces aanpak problematische jeugdgroepen en groepsgedrag: Het 7-stappenmodel, juni 2023.	

12. Rechten van betrokkenen

In iedere eenheid worden de verzoeken voor rechten van betrokkenen behandeld door de privacydesk. In dit onderdeel komt aan bod hoe de verwerkingsverantwoordelijke zorgdraagt voor de landelijke uitvoering van rechten betrokkene voor deze verwerking.

Uitvoering rechten betrokkene	Ja	Nee	Toelichting
De portefeuille beschikt over een landelijk protocol om een verzoek voor rechten betrokkene uniform te behandelen, voor de verwerkingen die onder diens verantwoordelijkheid vallen.		X	Verzoeken worden via de privacy-desk afgedaan.
De verwerkingsverantwoordelijke heeft een ingericht proces dat aansluit op de privacy desk		X	Er is geen ingericht proces, verzoeken worden door de privacy-desk afgehandeld.
De systemen zijn in staat om bijv. data te verwijderen of inzage te verlenen	X		Er kan eenvoudig op individueel niveau achterhaald worden welke informatie over een betrokkene geregistreerd is.
De verwerkingsverantwoordelijke is ingesteld om te voldoen aan het recht op informatie aan de betrokkene in o.a. een toegankelijke vorm.	X		Via de privacy-desk

B. Beoordeling rechtmatigheid gegevensverwerking

Beoordeling aan de hand van de feiten zoals vastgesteld in onderdeel A of de (voorgenomen) gegevensverwerking rechtmatig is. De juridische rechtsgrond, noodzaak en doelbinding van de gegevensverwerking zijn onderdeel van de beoordeling. Ook de wijze waarop invulling wordt gegeven aan de rechten van de betrokkenen blijft niet onbesproken.

13. Wettelijke doeleinden

Onderstaand de wettelijke doeleinden (politietaken) waarop de gegevensverwerking is gericht. Deze doeleinden moeten aan wettelijke voorwaarden voldoen, beoordeeld wordt hoe aan deze voorwaarden wordt voldaan.
De mogelijke wettelijke doeleinden zijn:

- Artikel 8 Wpg (uitvoering van de dagelijkse politietaak)
- Artikel 9 Wpg (onderzoek i.v.m. de handhaving van de rechtsorde in een bepaald geval)
- Artikel 10 Wpg (inzicht betrokkenheid van personen bij:
  - a) het beramen of plegen van misdrijven;
  - b) bepaalde ernstige bedreigingen van de rechtsorde;
  - c) ernstige schending van de openbare orde.)
- Artikel 12 Wpg (informanten)
- Artikel 13 Wpg (ondersteunende taken, schriftelijke vastlegging vereist)
- Artikel 22 Wpg (wetenschappelijk onderzoek en statistiek)

Voor de verwerking relevante doeleinden

Wettelijke doeleinden	Toetsing
Art. 8 Wpg	Het bestrijden en voorkomen van overlast door problematische jeugd en het meewerken aan het verzorgen van de juiste zorg voor problematische jeugd valt onder de dagelijkse politietaak ex art. 8 Wpg. Ook het op later tijdstip raadplegen van de aangemaakte AOPs en AOLs valt onder de art. 8 Wpg.
Art. 13 Wpg	Het aanmaken van de AOP en AOL zijn art. 13 Wpg verwerkingen.

14. Bijzondere politiegegevens

In deel A is beschreven of en welke bijzondere politiegegevens worden verwerkt. Het verwerken van bijzondere politiegegevens hoort uitsluitend plaats te vinden als dit onvermijdelijk is voor het doel van de verwerking, een aanvulling is op de verwerking van andere politiegegevens betreffende de persoon en de gegevens afdoende zijn beveiligd, art. 5 Wpg.

Beoordeel of de verwerkte bijzondere politiegegevens voldoen aan de vereisten van artikel 5 Wpg:

Wettelijke eis	Toetsing
De aangegeven te verwerken bijzondere politiegegevens zijn onvermijdelijk voor het doel	Om de juiste hulp (ketenpartners) voor een individu in te kunnen schakelen is het van belang dat de informatie over eventuele medische-, psychische-, of verslavingsproblematiek bekend is. Hetzelfde geldt voor het ter beschikking stellen van informatie aan de politieagent op straat die een individu benadert, deze informatie is van belang voor de veiligheid van zowel de agent als de betrokkene.
De te verwerken bijzondere politiegegevens zijn een aanvulling op de andere politiegegevens	De bijzondere politiegegevens worden verwerkt in combinatie met informatie over overlast en biografische informatie over de betrokkenen.
De te verwerken bijzondere politiegegevens zijn afdoende beveiligd	De bijzondere politiegegevens worden in 5.1.2.l en BVH verwerkt. 5.1.2.l scoort onvoldoende in het volwassenheidsniveau op basis van de Privacy & Security by Design 0-meting van 2019.[11] Dit betekent dat de politiegegevens onvoldoende veilig verwerkt worden.

15. Verdere verwerkingen

Politiegegevens kunnen verder worden verwerkt, namelijk in combinatie met elkaar en kunnen ter beschikking worden gesteld mits wordt voldaan aan de wettelijke vereisten in artikel 15 en 15a Wpg.

[11] Bijlage 1: 0-Meting Privacy & Security by Design 5.1.2.l, 2 april 2019.

In het geval dat een verdere verwerking plaats vindt wordt onderstaand beoordeeld of aan de wettelijke vereisten is voldaan:

Verdere verwerkingen	Toetsing
Artikel 8, derde, vierde lid Wpg	Verzamelde gegevens in het kader van de aanpak problematische jeugd kunnen worden meegenomen in een onderzoek zoals bedoeld in art. 9 of 10 Wpg of in het kader van informatenbeheer (art. 12 Wpg). Dit gebeurt echter niet structureel met alle geregistreerde individuen binnen de problematische jeugdgroepen.
Artikel 9, derde lid Wpg	n.v.t.
Artikel 10, vijfde lid Wpg	n.v.t.
Artikel 12, tweede, vierde lid Wpg	n.v.t.
Artikel 13	Het is onduidelijk of er een geldig art. 13 protocol ex art. 13 lid 4 Wpg jo. art. 6:2 Bpg is.

16. Autorisaties

Iedere verwerking van politiegegevens dient te voldoen aan het systeem van autorisaties zoals bedoeld in artikel 6. De terbeschikkingstelling van politiegegevens hangt samen met de autorisaties.

Hier wordt beoordeeld of de verwerking voldoet aan de voorwaarden voor autorisaties

De verwerking voldoet niet aan de eisen zoals deze volgen uit art. 6 Wpg.

17. Verstrekkingen aan externe partijen

De Wpg is een gesloten systeem voor de verstrekkingen aan partijen buiten het politiedomein. Per externe partij moet de verstrekking worden beoordeeld.

Beoordeel of de verstrekkingen aan externe partijen voldoen aan de wettelijke vereisten.

- Verstrekking aan gezagsdragers: artikel 16 Wpg
- Verstrekking aan inlichtingendiensten: artikel 17 Wpg
- Verstrekking aan derden structureel: artikel 18 Wpg
- Verstrekking aan derden incidenteel: artikel 19 Wpg
- Verstrekking aan derden structureel voor een samenwerkingsverband: artikel 20 Wpg
- Rechtstreekse verstrekking: artikel 23 Wpg
- Rechtstreekse verstrekking aan inlichtingen- en veiligheidsdiensten: artikel 24 Wpg

Opmerking: In het zorg & veiligheidsdomein heeft de Politie binnen de verschillende eenheden en regio's te maken met een grote verscheidenheid aan partijen. Deze partijen worden in deze GEB onderverdeeld in verschillende categorieën zodat het mogelijk blijft om bredere observaties te doen in plaats van specifiek op één district te focussen. Onderstaande tabel geeft de grondslagen van de verstrekkingen uitgesplitst in soort overlegstructuur.

De ketenpartners bij de incidentele en structurele overleggen worden uitgenodigd op basis van relevantie tot de te behandelen casus. Dit betekent dat er steeds sprake kan zijn van verschillende samenstellingen.

Externe partij	Toetsing grondslag verstrekking
Burgemeester (gezagsdrager)	De politiegegevens over problematische jeugdgroepen zien op de handhaving van openbare orde. Deze verstrekking is gerechtvaardigd. (art. 16 Wpg)
Officier van Justitie	In de driehoek worden de gegevens gedeeld vanwege de rol van het OM in de zeggenschap en de beheertaak. (art. 16 Wpg)
Derden incidenteel	Verstrekkingen bij incidentele overleggen vinden plaats op grond van art. 19 Wpg. Een verstrekking op basis van art. 19 Wpg wordt door de ABRvS als een besluit in de zin van de Awb (art. 1:3 lid 1) aangemerkt.[12] Dit betekent dat de betrokkene de gelegenheid moet krijgen om een zienswijze in te dienen op het voorgenomen besluit.[13] Aan dit vereiste wordt in de praktijk niet voldaan tenzij er sprake is van een spoedeisend belang.[14] De politiegegevens worden dan door de wijkagent verstrekt in incidentele overleggen met ketenpartners. De wijkagent maakt een I90-formulier op na de verstrekking waarin de verstrekking wordt vastgelegd en gelegitimeerd. Art. 19 Wpg wordt uitsluitend in incidentele (uitzonderings-)gevallen gebruikt waarbij er (nog) geen art. 20 Wpg-beslissing met bijbehorend convenant is en is geen geschikte grondslag voor een structurele of voorzienbare verstrekking aan derden.
Derden structureel samenwerkingsverband	Voor de verstrekking aan het Zorg en Veiligheidshuis en andere vaste overlegstructuren wordt gebruik gemaakt van een art. 20 Wpg beslissing in combinatie met een convenant.[15] Het zwaarwegend algemeen belang bestaat uit het handhaven van de openbare orde en het verlenen van zorg aan hen die deze behoeven. De verstrekking gaat gepaard met het opmaken van een I90-formulier waarin de verstrekking wordt vastgelegd en gelegitimeerd.

Algemene opmerking ten aanzien van verstrekkingen

Het is aan de verstrekkende politieambtenaar om te beoordelen of een politiegegeven relevant is voor het doel van de verstrekking aan de ketenpartners(s). Er wordt daarbij voor wat betreft de aanpak van problematische jeugd steeds een beroep gedaan op het inschattingsvermogen van de individuele politieambtenaar (de wijkagent of de OSB Z&V). Er is geen landelijk kader voor de inhoudelijke beoordeling van een dergelijke verstrekking. Dit werkt een

---

[12] ABRvS 15 mei 2015, ECLI:NL:RVS:2015:1504. (link)
[13] Art. 4:7 Awb.
[14] Bij een spoedeisend belang voorziet art. 4:11 sub a Awb in een uitzonderingsgrond op art. 4:7 Awb.
[15] Zie Modelconvenant Jeugdgroepaanpak. 3 oktober 2022 (opgesteld door: Ministerie van Justitie en Veiligheid, Politie, Openbaar Ministerie, VNG).

situatie in de hand waarbij verstrekkingen verschillend verlopen in verschillende regio's. Bovendien staat niet vast of een individuele politieambtenaar over voldoende context beschikt om in alle gevallen een gedegen afweging te maken om al dan niet over te gaan tot verstrekking of achterwege houden van (delen van) politiegegevens.

18. Doorgifte aan derde landen

Hieronder wordt de doorgifte van politiegegevens aan derde landen getoetst aan de hand van artikel 17a Wpg.

Naam derde landen	Toetsing doorgifte
-	Er vindt geen doorgifte plaats.

19. Noodzakelijkheid, rechtmatigheid en doelbinding

Politiegegevens worden slechts verwerkt als dit noodzakelijk is voor de wettelijke doeleinden, behoorlijk en rechtmatig is, de gegevens rechtmatig zijn verkregen, gelet op de doeleinden toereikend, ter zake dienend en niet bovenmatig zijn, artikel 3 lid 1 en 2 Wpg.

19a. In dit onderdeel wordt beoordeeld of de verwerking en de verdere verwerkingen zoals terbeschikkingstellingen en verstrekkingen voldoen aan de criteria van noodzakelijkheid, rechtmatigheid en doelbinding:

Er is geen data over de daadwerkelijke effectiviteit van de aanpak. Bij de beoordeling wordt uitgegaan van vigerend beleid en de manier waarop de processen op dit moment invulling hebben gekregen.

Criteria	Verwerking
Proportionaliteit *Staat het belang van de verwerking in verhouding tot de inbreuk op de persoonlijke levenssfeer?*	De verwerking heeft als grootste belang het handhaven van de openbare orde, het verzorgen van (geleiden naar) de juiste zorg en voorkomen van overlast door problematische jeugdgroepen door middel van het toepassen van een passende aanpak. Problematische jeugdgroepen kunnen een grote impact hebben op de openbare orde en serieuze overlast veroorzaken. In het geval dat dit in het jongerentafeloverleg vastgesteld wordt, geeft dit een belang dat zwaar genoeg weegt voor het in kaart brengen van de groep door middel van het uitvoeren van een groepsscan. Na de identificatie van de groepsleden kan de daadwerkelijke aanpak bepaald worden. Dit resulteert voor de Politie in informatie over zowel de bejegening van de groep als geheel als de individuen binnen die groep. Dit heeft als doel om de betrokken individuen zo effectief mogelijk te doen ophouden met het veroorzaken van overlast of het verstoren van de openbare orde. Het is in het belang van zowel de leden van de jeugdgroep als de politieambtenaar dat de leden van de jeugdgroep gepast bejegend worden. Hoewel de delen van het opgestelde handelingskader die door de Politie worden verwerkt eventueel gegevens kunnen bevatten welke een inbreuk kunnen vormen op de persoonlijke levenssfeer van het individu levert de uiteindelijke toepassing van dit handelingskader een betere situatie op voor zowel de betrokkene als de politieambtenaar. De verwerking is dus proportioneel.
Subsidiariteit *Zijn andere minder in de persoonlijke levenssfeer van de burger ingrijpende maatregelen mogelijk?*	Voor het analyseren van een jeugdgroep is het opmaken van een groepsscan het aangewezen middel omdat met het resultaat de 'zwaarte' van een groep kan worden vastgesteld. Daarom is het van belang dat de soorten delicten worden uitgesplitst. Ook is het voor de aanpak van belang om te zien binnen welk geografisch gebied een groep actief is. Er is geen mogelijkheid om hetzelfde informatieproduct met minder gegevens tot stand te brengen. Als de handelingskaders op een professionele manier worden opgesteld is het onwaarschijnlijk dat er minder gegevens kunnen worden verwerkt om hetzelfde doel te bereiken. Er wordt gedifferentieerd tussen de aanpak op individueel niveau en het groepsniveau.
Niet bovenmatig *Is de verwerking niet bovenmatig en niet meer dan nodig voor het doel?*	Als er gehandeld wordt zoals beschreven in onderdeel A.1. worden er niet meer politiegegevens verwerkt dan noodzakelijk.

19b. Verkrijging van de verkrijging
Onderstaand wordt getoetst of de oorsprong van de gebruikte politiegegevens rechtmatig is.

Toetsing
De politiegegevens worden verkregen uit het dagelijkse politiewerk. Of dit dagelijkse politiewerk in individuele cases rechtmatig plaatsvindt is geen onderdeel van de beoordeling. Nieuwe informatie ten opzichte van bejegening volgt uit gesprekken met ketenpartners. Op welke wijze ketenpartners deze informatie verkregen hebben, valt buiten de scope van deze GEB.

20. De verwerker
De politie kan een verwerker inschakelen om politiegegevens onder het gezag van de politie te verwerken (artikel 6c Wpg).

20a. Verwerkers
De politie maakt in deze verwerking geen gebruik van verwerkers.

20b. Van toepassing zijnde verwerkersovereenkomst(en)
Geen verwerkersovereenkomsten

21. Beoordeling verwerkingstermijnen
In dit onderdeel worden de verwerkingstermijnen van artikel 8, 9, 10, 12 en 13 Wpg getoetst.

21a. De feitelijke hantering van verwerkingstermijnen zoals genoemd in deel A en de wettelijke termijnen.

Wettelijke politietaak Art. 8, 9, 10, 12 of 13 Wpg	Wettelijke termijn	Feitelijke termijn	Toetsing
Art. 8	Eén jaar vrij opvraagbaar, vier jaren voor geautomatiseerde vergelijking beschikbaar.	De gegevens van betrokkenen die in 5.1.2.I aan een groep zijn toegevoegd worden de facto langer bewaard dan de in art. 8 genoemde termijnen. De groepen moeten namelijk handmatig worden verwijderd. In de praktijk gebeurt dit niet tijdig.	De verwerking voldoet niet aan de verwerkingstermijnen die volgen uit art. 8 Wpg.
Art. 13	Er moet een verwerkingstermijn worden vastgesteld in een art. 13 protocol ex art. 13 lid 4 Wpg jo. art. 6:2 lid 1 sub c Bpg.	Het is op dit moment niet duidelijk of er een art. 13-protocol in werking is. De AOL en AOP worden op dit moment maximaal vijf jaren verwerkt waarna ze verwijderd worden. Het is onduidelijk of de AOL en AOP ook vernietigd worden.	Niet compliant vanwege het ontbreken van een art. 13 protocol. Ook staat niet vast dat de AOP en AOL tijdig vernietigd worden.

21b. Beantwoord deze vraag in het geval er sprake is van een verwerking voor ondersteunende taken, artikel 13 verwerking.

Is er een schriftelijke vastlegging waar de verwerkingstermijn in beschreven staat? Beschrijf de inhoud van de vastlegging en voeg deze toe.

Antwoord:

Er is geen schriftelijke vastlegging zoals bedoeld in art. 13 lid 4 Wpg jo. art. 6:2 Bpg.

22. Rechten van betrokkenen

Uitvoering rechten betrokkene	Beoordeling
De portefeuillehouder beschikt over een protocol om een verzoek omtrent rechten betrokkene uniform te behandelen	Er is geen protocol voor de afhandeling van verzoeken van betrokkenen.
De gemandateerd verwerkingsverantwoordelijke heeft een ingericht proces dat aansluit op de privacy desk	Er is geen specifieke aansluiting op de privacy-desk. De reguliere processen van de privacy-desk sluiten aan op de aanpak van problematische jeugdgroepen.
De systemen zijn in staat om bijv. data te verwijderen of inzage te verlenen	De systemen zijn in staat op data te verwijderen en inzage te verlenen.
De gemandateerd verwerkingsverantwoordelijke is ingesteld op het recht op informatie aan de betrokkene in o.a. een toegankelijke vorm.	Blijkt niet uit de gesprekken of stukken.

C. Risico's

Thema	#	Risico omschrijving voor betrokkene en/of organisatie	Kans	Impact	Risico Inschatting	Maatregelen	Restkans	Restimpact	Restrisico inschatting
1. Organisatie	1.2. Rechtmatigheid	[redacted]	4	4	16	Beschrijf de verwerking voor de ondersteuning van de politietaak om de verwerking te reguleren.	1	1	1
1. Organisatie	1.5. Werkproces	[redacted]	5	3	15	Onderzoek hoe de landelijke uniformiteit kan worden verbeterd. Bijvoorbeeld door: - Controleer de landelijke werkinstructies op naleving. - Pas waar nodig werkinstructies aan. - Actualiseer het [redacted].	1	3	3
1. Organisatie	1.5. Werkproces	[redacted]	4	4	16	[redacted]	1	1	1

						[redacted]			
1. Organisatie	**1.7. Autorisatie**	Autorisaties worden niet periodiek gecontroleerd. [redacted]	5	3	15	Zorg voor [redacted] en reguliere controle van de autorisaties volgens het beleid of autorisatiematrix. Of ontwerp de nieuwe applicatie [redacted] zodanig dat deze geschikt is voor periodieke (geautomatiseerde) controle.	1	3	3
1. Organisatie	**1.7. Autorisatie**	De controle op de autorisatie voor [redacted] vindt onvoldoende plaats omdat [redacted]	5	3	15	Benoem [redacted] als applicatie waarvoor controle [redacted] plaats vindt, meld deze bij de FG, vraag aan de productowners wat er voor nodig is om dit gebruikersvriendelijker te maken. Of ontwerp de nieuwe applicatie [redacted] zodanig dat deze geschikt is voor periodieke (geautomatiseerde) controle.	1	3	3

1. Organisatie	**1.8. Verwerkings termijnen**	Vanwege de inrichting van 5.1.2.I in combinatie met de brief van de Minister van Justitie en Veiligheid inzake cold cases worden gegevens niet tijdig vernietigd. Ook worden registraties van jeugdgroepen niet tijdig verwijderd / opgeschoond. De verwerkingstermijnen worden niet nageleefd waardoor de verwerking langer plaatsvindt en de gegevens langer toegankelijk zijn dan is toegestaan.	5	5	25	Pas systemen en procedures aan om de verwerkingstermijnen na te leven. Geef de medewerkers de nodige instructies.	1	1	1
4. Technische aspecten	**4.1. Logging**	5.1.2.I voldoet niet aan de vereisten voor logging, de audittrail van een record kan worden aangepast door de beheerder.	3	3	9	Pas het beleidskader logging en monitoring toe op 5.1.2.I.	1	1	1
4. Technische aspecten	**4.3. Doel applicatie**	De verwerking maakt gebruik van 5.1.2.I, een applicatie niet voldoet aan het vigerende beleid.	5	2	10	Maak gebruik van het Portaal Bestandsuitwisseling bij de uitwisseling van bestanden tussen Politie en ketenpartners.	1	2	2
5. Externe partijen	**5.1. Grondslag**	De incidentele verstrekking op basis van art. 19 Wpg in die gevallen dat er geen sprake is van een spoedeisend belang voldoet niet aan de wettelijke vereisten die	2	3	6	Geef de betrokkene de gelegenheid om een zienswijze naar voren te brengen of gebruik art. 19 uitsluitend als	1	1	1

		volgen uit de Awb. De betrokkene wordt de gelegenheid ontzegd om zijn zienswijze te geven op de voorgenomen verstrekking.				verstrekkingsgrond in spoedeisende gevallen.			
5. Externe partijen	**5.1. Grondslag**	Verstrekkingen worden door individuele politieambtenaren beoordeeld. Dit leidt mogelijk tot verschillen in de verstrekkingen per regio. Ook is er geen landelijk kader dat de verstrekkingen regelt.	5	2	10	Stel een landelijk kader op dat richting geeft aan de verstrekkingen.	1	1	1

Bijlagen

Bijlage 1 – 0-Meting Privacy & Security by Design [redacted], 20 april 2019.

Gegevensbeschermings effectbeoordeling (GEB) Wpg

Uitvoeren identiteits-onderzoek (1e lijns)

Gegevensbeschermingseffectbeoordeling Wet politiegegevens

Definitief

Versie: 1.0

Versie datum: 7 oktober 2024

Versiegeschiedenis

Versie	Versie datum	Samenvatting van de aanpassing	Gemarkeerde wijzigingen
01	20-06-2023	Eerste concept	N.v.t
02	28-07-2023	Tweede concept n.a.v. aanpassingen 1e review	Zie versie 0.1
03	28-11-2023	Derde concept n.a.v. aanpassen 2e review	Zie versie 0.2
1.0	04-07-2024	Definitief	N.a.v. review versie 0.3

Distributie

Versie	Verzend datum	Naam	Afdeling / Functie
0.3	18-12-2023	5.1.2.e	Landelijke Eenheid, Privacyfunctionaris

Review commentaar

Versie	Wanneer	Wie	Functie
0.1		5.1.2.e	Adviseur privacy
0.2		5.1.2.e	Adviseur privacy
0.3		5.1.2.e	Privacyfunctionaris

Inhoudsopgave

Basisinformatie

Naam van de verwerking zoals aangemeld in 5.1.2.i	Uitvoeren identiteitsonderzoek (1e lijns)
Ingangsdatum van de verwerking	Bestaande verwerking
Gemandateerd verwerkingsverantwoordelijk Portefeuillehouder en eenheid	Portefeuille GGP, Portefeuillehouder Yvonne Hondema.
Politie onderdeel waar de verwerking plaatsvindt	Het proces wordt door vrijwel de hele operatie uitgevoerd.
Contactpersoon m.b.t. deze verwerking	5.1.2.e portefeuille GGP
Privacyfunctionaris	5.1.2.e

Betrokken bij deze GEB	**Naam**
Privacy adviseur	5.1.2.e (penvoerder) 5.1.2.e (reviewer en penvoerder ID-onderzoeken in het kader van de openbare orde)
Reviewrol privacy adviseur	5.1.2.e
IB Analist hulpstructuur privacy	5.1.2.e (IB)
Privacyfunctionaris portefeuille	5.1.2.e
Adviseur portefeuillehouder	5.1.2.e
Materiedeskundigen	5.1.2.e, Operationeel Specialist C, Team Politieprofessie (DH), 5.1.2.e, Operationeel Specialist B, 5.1.2.e, Operationeel Specialist B

Functionaris Gegevensbescherming	
FG:	5.1.2.e en 5.1.2.e 5.1.2.i @politie.nl
Advies nodig: ja/nee	Ja
Toelichting: De GEB Uitvoeren identiteits-onderzoek (1e lijns) versie 1.0 is op 5 juli 2024 ter advies aan de FG voorgelegd. De FG heeft op basis van de GEB een beeld kunnen vormen van de voorgenomen verwerkingen die plaatsvinden in het kader van het 1e-lijns identiteitsonderzoek. Wel merken we op dat de omschrijving van risico's 1 + 2 onder 'organisatie' gebaat is bij herformulering; in hoeverre is de rechtmatigheid hier in het geding en hoe verhouden deze zich tot elkaar en/of andere genoemde risico's? We vragen bijzondere aandacht voor het issue rondom ID-controles in het kader van openbare orde. We adviseren hier een specificering aan te brengen voor ID-controles bij demonstraties en vragen om als risico uitdrukkelijker de mogelijke inperking van dit grondrecht in beeld te brengen; de algemene instructies volstaan in dit verband niet als maatregel. Omdat deze GEB ziet op een bestaande verwerking ten aanzien waarvan nog niet alle beschreven maatregelen zijn doorgevoerd, verzoeken we de gemandateerd verantwoordelijke om in Q4 2024 een overzicht van de voortgang van de feitelijke risico mitigatie aan te leveren.	

Gezien door verwerkingsverantwoordelijke

Naam	Yvonne Hondema (GGP)
Functie	Portefeuillehouder GGP
Datum	
Opmerkingen: Ondertekening ter vaststelling van de inhoud van de GEB en kennisneming van het FG-advies door de (gemandateerd) verwerkingsverantwoordelijke.	

1. Managementsamenvatting

1.1. Hoog risico verwerking

Deze managementsamenvatting van de gegevensbeschermingseffectbeoordeling (hierna: GEB) is bedoeld voor besluitvorming door de verwerkingsverantwoordelijke. Het bevat de belangrijkste bevindingen, risico´s en maatregelen voor de onderzochte verwerking.
Op de verwerking van de portefeuille zijn een GEB en een informatiebeveiligingsanalyse uitgevoerd op grond van de Wet politiegegevens (hierna: Wpg). Een GEB wordt uitgevoerd als een gegevensverwerking waarschijnlijk een hoog privacy-risico oplevert voor de personen over wie de politiegegevens verwerkt.

De criteria voor een hoog risico-verwerking zijn bepaald door de Europese toezichthouder en het beleid van de politie. Deze criteria zijn opgenomen in de 'quickscan' die wordt uitgevoerd in het systeem 5.1.2.i. Hier vindt ook de registratie van de verwerking plaats. De criteria voor de hoog risicoverwerkingen zijn opgenomen in de toelichting bij het GEB-formulier.

De verwerking is als een hoog risicoverwerking aangemerkt omdat:

De Europese toezichthouder EDPB (European Data Protection Board) heeft een negental criteria opgesteld, waarbij als vuistregel geldt dat een GEB dient te worden uitgevoerd als de verwerking aan twee of meer van deze criteria voldoet. De hoofdverwerking waar deze GEB op ziet voldoet aan de volgende criteria, namelijk:

1. Het verwerken van gevoelige gegevens zoals biometrische gegevens (biometrische gelaatsfoto's & vingerafdrukken);
2. Er is sprake van grootschalige gegevensverwerkingen. (o.a. 1,3 miljoen registraties in de HAVANK-database en de overige dagelijkse identiteitsonderzoeken.)
3. Bij het vaststellen van de identiteit of het verifiëren van de identiteit van verdachten met behulp van de technische voorziening, (de ID-zuil) worden de ingevoerde (politie)gegevens gecombineerd en gekoppeld met meerdere databronnen.

1.2. Aanpak

Deze GEB is tot stand gekomen in overleg met de adviseurs van de portefeuille GGP en de aangewezen materiedeskundigen uit de operatie. Betrokken bij de uitvoering waren:
- de adviseurs privacy: 5.1.2.e (penvoerder) en 5.1.2.e (reviewer en penvoerder ID-onderzoeken eerste lijns in het kader van de openbare orde);
- de IB-analist: 5.1.2.e;
- de materiedeskundigen: 5.1.2.e, 5.1.2.e en 5.1.2.e.

De aanpak was als volgt:

<u>Voor wat betreft de ID-onderzoeken in de strafrechtketen</u>
Als eerste is een verkennend gesprek met de materiedeskundige gevoerd. Hiermee is een eerste indruk verkregen van de manieren waarop de identiteit van een verdachte met behulp van ID-zuil kan worden vastgesteld. Ook is toegelicht in welke gevallen de ID-zuil wordt gebruikt. Vervolgens is met behulp van het 'Protocol Identiteitsvaststelling Strafrechtketen 2020' (zie bijlage) is de uniforme werkwijze beschreven die van toepassing is bij de vaststelling van de identiteit van verdachten.[1] Dit protocol is vervolgens getoetst aan de uitvoeringspraktijk. De documenten zijn als bijlage toegevoegd.

<u>Voor wat betreft ID-onderzoeken in het kader van de openbare orde zonder verdenking van een strafbaar feit</u>
Naar aanleiding van het rapport 'Ongecontroleerde macht' van Amnesty International is de scope van de GEB uitgebreid met de geconstateerde werkwijze op basis van art. 3 Pw 2012 waarbij geen verdenking bestaat van een strafbaar feit. Er hebben, gezien de complexiteit van de materie, meerdere gesprekken plaatsgevonden om het proces inzichtelijk te krijgen. Hierbij heeft de focus, gezien de expertise en de hoeveelheid van demonstraties, gelegen op de eenheid Den Haag.

[1] Het 'Protocol Identiteitsvaststelling Strafrechtketen 2020', is opgesteld door het Ministerie van Justitie en Veiligheid.

1.3. Belangrijkste bevindingen verwerking

Korte beschrijving van de belangrijkste aangetroffen privacy en IB-issues:

1. Issue: De verwerking voor ondersteuning van de politietaak (art. 13 Wpg) heeft geen schriftelijke vastlegging van de frequentie waarmee de verwerkingstermijnen van de gegevens worden gecontroleerd.
   Risico: Hierdoor is de verwerking niet conform wet- en regelgeving en loopt de betrokkene het risico dat o.a.: er te veel gegevens worden verwerkt, dreigt voor de organisatie stopzetten van de verwerking, een boete en imagoschade.
   Maatregel: Beschrijf in een addendum de frequentie waarop de verwerkingstermijnen van de gegevens in de HAVANK-strafrechtdatabase en voor de identiteit van personen gecontroleerd worden en stel dit vast als onderdeel van het art. 13 protocol.

2. Issue: Autorisaties die verleend zijn via 5.1.2.i worden niet altijd periodiek gecontroleerd.
   Risico: 5.1.2.i
   Maatregel: Controleer de autorisaties periodiek en borg dit binnen de werkprocessen 5.1.2.i

3. Issue: Er is geen vastgesteld werkproces en/of protocol om ID-controles uit te voeren indien dit specifiek gaat om de handhaving van de openbare orde. Derhalve worden de controles mogelijk niet altijd conform wet- en regelgeving uitgevoerd.
   Risico: Mogelijk onrechtmatige gegevensverwerking, reputatieschade en boetes.
   Maatregel: Stel een werkproces/protocol op zodat in de operatie duidelijkheid bestaat omtrent het juridisch en beleidsmatig kader.

4. Issue: Voor een artikel 13 lid 1 Wpg verwerking ontbreekt een schriftelijke vastlegging van de verwerkingstermijn.
   Risico: De duur van de verwerking is hierdoor onbepaald wat kan leiden tot misbruik van gegevens.
   Maatregel: Bepaal de verwerkingstermijnen en zorg voor een schriftelijke vastlegging en geef instructies aan de medewerkers om hier uitvoering aan te geven.

1.4 Vervolgproces

Het vervolgproces voor de portefeuillehouder ten aanzien van de maatregelen:

De GEB beschrijft de maatregelen die nodig zijn om de risico's te mitigeren die volgen uit de bevindingen ten aanzien van de verwerking Uitvoeren identiteitsonderzoek (1e lijns).

De portefeuille GGP heeft de taak deze mitigerende maatregelen te implementeren of een (rest)risico te accepteren. Daarom dient na de ondertekening van de GEB een besluitvormingstraject over de mitigerende maatregelen te volgen. De portefeuillehouder is verantwoordelijk voor een plan van aanpak om de implementatie van de maatregelen te realiseren.

Met betrekking tot individuele applicaties kan bij het de hulpstructuur privacy nadere informatie worden aangevraagd, zoals uitgevoerde IB–analyses.

A. Beschrijving kenmerken gegevensverwerking

1. Beschrijving verwerking

Een ieder is, aldus art. 2 van de Wet op de identificatieplicht, gehouden om een identiteitsbewijs te kunnen tonen aan onder andere de politie. De politie voert in het kader van de uitoefening van de politietaak van de politie, gecodificeerd in art. 3 Politiewet 2012 (Pw 2012) identiteitsonderzoeken uit. De identiteitsonderzoeken kunnen zowel uitgevoerd worden in het kader van strafrechtelijke handhaving of ter voorkoming van wanordelijkheden ten aanzien van de openbare orde.

Deze GEB maakt inzichtelijk welke politiegegevens worden verwerkt bij het vaststellen of verifiëren van de identiteit van een betrokkene. De politie stelt de identiteit, indien nodig, vaak vast tijdens het eerste contact met de betrokkene op straat. Daarbij wordt de identiteit meestal geverifieerd aan de hand van een identiteitsbewijs als bedoeld in art. 1 van de Wet op de Identificatieplicht (denk hierbij aan een paspoort en/of identiteitskaart). De politie toetst het door de betrokkene overgelegde identiteitsbewijs op een aantal echtheidskenmerken en door middel van verificatie in de politiesystemen. Bij een positieve identificatie zal de politie eventuele vervolgstappen bepalen. Dit kan onder andere het geven van een waarschuwing of aanwijzing zijn maar ook het opleggen van een sanctie of het doen van een aanhouding. Bij de verificatie in politiesystemen wordt o.a. gebruik gemaakt van de applicaties 5.1.2.1, BVH en MEOS. Indien er na de controle van het document en de verificatie in de politiesystemen twijfel bestaat over de identiteit van een verdachte kan deze worden aangehouden. Na de aanhouding volgt de identificatie of verificatie van de identiteit van de verdachte met behulp van de ID-zuil waarbij biometrische gegevens gebruikt worden om tot identificatie te komen.

Met de invoering van de Wet identiteitsvaststelling verdachten, veroordeelden en getuigen (Wivvg) is het vaststellen van de identiteit van verdachten, veroordeelden en getuigen in de strafrechtketen een wettelijke verplichting.[2] Het 'Protocol Identiteitsvaststelling Strafrechtketen' geeft aan die wettelijke verplichting nadere invulling.

Gegevensverwerking door de ID-zuil

De ID-zuil is aangesloten op primaire en secundaire registers (zie bijlage I). Binnen de strafrechtketen is de ID-zuil gekoppeld aan drie databanken: Het Automatisch Vingerafdrukken Systeem Nederlandse Kollektie (HAVANK), Voorziening voor verificatie en identificatie (VVI) en strafrechtketendatabank (SKDB). Met behulp van de ID-zuil kunnen verschillende (persoons)gegevens gekoppeld worden[3]. Het identiteitsbewijs kan worden gescand en – als een chip aanwezig is – kan deze worden uitgelezen. Met behulp van de ID-zuil kunnen vingerafdrukken en gelaatsfoto's van verdachten worden afgenomen. Identificatie en verificatie met behulp van de ID-zuil kan alleen plaatsvinden als de verdachte al bekend is binnen de SKDB.[4] Indien bij het gebruik van de ID-zuil blijkt dat de verdachte nog geen Strafrechtketennummer (SKN) heeft zal de verdachte worden gekoppeld en wordt daarmee opgenomen in de SKDB.

Gegevensverwerking in het kader van de handhaving van de openbare orde zonder verdenking van een strafbaar feit

In art. 11 van het Europees Verdrag voor de Rechten van de Mens (EVRM) en art. 9 van de Grondwet is het demonstratierecht verankerd. Iedereen heeft het recht om te demonstreren maar dit recht is niet absoluut. Het recht op demonstratie kan dus ook begrensd worden indien dit noodzakelijk is. Het begrenzen van dit recht kan bijvoorbeeld plaatsvinden bij een wanordelijkheid ten aanzien van de openbare orde en veiligheid. Het bevoegd gezag toetst in zo'n geval of het beperken van het demonstratierecht noodzakelijk is. De politie heeft hierin een uitvoerende en toezichthoudende rol. Soms is het ook nodig dat de politie, in opdracht van het bevoegd gezag, demonstraties daadwerkelijk begrenst of beëindigt door middel van actief optreden.

Wanneer de politie aanwezig is bij demonstraties kan, indien dit noodzakelijk is ter uitvoering van de politietaak, worden overgegaan tot het identificeren van betrokkenen. Het verrichten van een identiteitsonderzoek in het kader van deze taakstelling (op basis van art. 3 Pw 2012) van de politie wordt geacht met terughoudendheid toegepast te worden.[5] Zo kan er tot identificatie worden overgegaan indien er sprake is van een mogelijk dreigende situatie of indien gemaakte afspraken met de demonstratieleiding worden geschonden. Indien er sprake is van een verdenking van een strafbaar feit tijdens een demonstratie wordt het reguliere proces gehanteerd.

---

[2] Stb. 2009, 317 en besluit identiteitsvaststelling verdachten en veroordeelden.

[3] De applicatie HAVANK is ondersteunend aan de verwerking, deze valt echter niet onder de (gemandateerde) verwerkingsverantwoordelijkheid van de portefeuillehouder GGP.

[4] Voor de strafrechtsketen wordt een centraal bestand van identificerende administratieve persoonsgegevens en foto's van verdachten en veroordeelden opgebouwd: de strafrechtsketendatabank (SKDB; zie artikel 27b, vierde lid Sv).

[5] College voor de Rechten van de Mens, Demonstratierecht onder druk, blijkt uit aanhouding klimaatactivisten, 31-01-2023.

Als een burger voornemens is om te gaan demonstreren kan er door de betrokkene voor worden gekozen om deze demonstratie aan te melden bij het bevoegd gezag zodat het bevoegd gezag eventueel maatregelen kan nemen en/of dit af kan stemmen met de politie. Door het aanmelden van een demonstratie wordt de politie de gelegenheid geboden om de risico's ervan in te schatten en maatwerk te leveren omtrent de inzet van politiemedewerkers om zodoende op een voorspelbare manier op te kunnen treden om zo de impact van de aanwezigheid van de politie te beperken. Ook wordt door het aanmelden mogelijk voorkomen dat er meer mensen dan noodzakelijk aan een identiteitsonderzoek worden onderworpen doordat de demonstratieleiding al bekend is bij de politie. Indien een demonstratie door de demonstratieleiding is aangemeld worden gegevens van de aanmelder vastgelegd in de Politiekalender, Live Journaal Politie (LJP) en/of op interne dashboards voor wat betreft de monitoring van demonstraties. Met de betrokkene(n) kan vervolgens afspraken worden gemaakt met betrekking tot bijv. de locatie en tijdsduur van de demonstratie en de beschikbaarheid van de politie.

Indien er sprake is van een niet aangemelde demonstratie worden in beginsel geen gegevens vastgelegd van de betrokkene. Wel wordt (door of namens de OVD-P), in opdracht van het bevoegd gezag, met de verondersteld demonstratieleider afspraken gemaakt met betrekking tot o.a. de locatie en tijdsduur. Indien er ernstige vrees bestaat voor wanordelijkheden en/of de demonstratieleider geen uitvoering geeft aan de gemaakte afspraken wordt tot identificatie en vastlegging overgegaan.
De overwegingen om tot identificatie over te gaan van deelnemers aan demonstraties hangt sterk af van de omstandigheden van het geval, hier is namelijk geen vastgesteld werkproces voor opgesteld waardoor onduidelijkheid bij collega's op straat bestaat omtrent de reikwijdte van de bevoegdheden.

Indien uit een risicobeoordeling blijkt dat de demonstratie een hoog risico op wanordelijkheden met zich meebrengt wordt bij afwijkend gedrag eerder tot identificatie overgegaan om zo een goed beeld te kunnen krijgen van de demonstratie en het bevoegd gezag te kunnen informeren. Als er een verhoogd risico bestaat zal er veelal een SGBO (Staf Grootschalig en Bijzonder Optreden) worden ingericht die de algehele inzet bij een demonstratie verzorgt.
Binnen een SGBO wordt door de hoofd intelligence een uitgebreide risico inschatting gemaakt door middel van rapportages waarop later geacteerd kan worden door de politie op straat. Dit acteren kan bijvoorbeeld zijn in de vorm van een ID-onderzoek van een betrokkene die afwijkend gedrag vertoont.

<u>Buiten de scope van deze GEB.</u>
De ID-zuil is een technische voorziening die binnen de strafrechtketen door de ketenpartners wordt gebruikt. Afbakening is daarom nodig. Ten eerste is het vaststellen van de identiteit van veroordeelden of getuigen geen politietaak en zij vallen daarom buiten de scope van deze GEB. Ook alle identiteitsvaststellingen op basis van de bestuursrechtelijke handhaving en DNA-afname vallen buiten de reikwijdte van deze GEB. Tot slot vallen de vreemdelingen die gecontroleerd worden op grond artikel 50 lid 1 Vreemdelingenwet, ter vaststelling van de nationaliteit en hun verblijfsrecht, niet onder de scope van deze GEB.[6] Indien een vreemdeling (ongeacht zijn verblijfstatus) echter door de politie wordt aangemerkt als een verdachte in de zin van artikel 27 lid 1 Sv valt de vreemdeling wel onder de reikwijdte van deze GEB. Immers als de vreemdeling als verdachte wordt aangemerkt is de politie wettelijk verplicht tot het vaststellen van de identiteit (met of zonder hulp van de ID-zuil) op grond van artikel 3 en 8 Pw 2012 en artikel 27a Sv.[7] Verder zijn er aparte GEB's en addenda uitgevoerd op het maken van de gelaatsfoto en het afnemen van vingerafdrukken. In deze GEB wordt verder niet ingegaan op deze onderwerpen en deze vallen buiten scope van de GEB Uitvoeren identiteitsonderzoek (1e lijns).

Tot slot valt het proces van de totstandkoming en het gebruik van de risicorapportages in het kader van de handhaving van de openbare orde buiten scope. Dit betreffen intelligence rapportages opgesteld door o.a. het Regionale Informatie- en Expertisecentra (RIEC), het Team Openbare Orde Inlichtingen (TOOI) en Open Source Intelligence (OSINT).

2. Big data

De verwerking voldoet niet aan kenmerken van Big Data verwerkingen. Zo is er bijvoorbeeld geen sprake van het combineren van zowel gestructureerde als ongestructureerde data uit verschillende bronnen.

---

[6] De ambtenaren belast met de grensbewaking en de ambtenaren belast met het toezicht op vreemdelingen, zijn bevoegd, hetzij op grond van feiten en omstandigheden die, naar objectieve maatstaven gemeten, een redelijk vermoeden van illegaal verblijf opleveren hetzij ter bestrijding van illegaal verblijf na grensoverschrijding, personen staande te houden ter vaststelling van hun identiteit, nationaliteit en verblijfsrechtelijke positie.

[7] Als verdachte wordt aangemerkt degene te wiens aanzien uit feiten of omstandigheden een redelijk vermoeden van schuld aan een strafbaar feit voortvloeit.

3. Motivering hoog risicoverwerking

De Europese toezichthouder EDPB (European Data Protection Board) heeft negen criteria opgesteld. Conform het Beleidskader Registerplicht en GEB geldt hierbij als vuistregel dat een GEB dient te worden uitgevoerd als de verwerking aan twee of meer van deze criteria voldoet. Op deze verwerking dient een GEB uitgevoerd te worden op basis van de volgende criteria:

- Verwerken van gegevens van gevoelige of bijzondere aard
- Grootschalige gegevensverwerkingen
- Ingevoerde politiegegevens worden gecombineerd en gekoppeld met meerdere databronnen

Bij het identificatieproces door middel van de ID-zuil kan er gebruik worden gemaakt van vingerafdrukken, dit betreffen biometrische gegevens. Biometrische gegevens vallen onder de categorie bijzondere politiegegevens.[8]
De vingerafdrukken zijn opgenomen in de HAVANK-strafrechtdatabase. Deze databank bevat de gegevens van ongeveer 1,3 miljoen betrokkenen. Tezamen met de overige controles resulteert dit in een verwerking op grote schaal. Zowel het aanhouden van de databank als het vergelijkend doorzoeken van de databank vormen verwerkingsactiviteiten die samen in ieder geval tot een grootschalige verwerking van politiegegevens leiden.
Bij het vaststellen van de identiteit of het verifiëren van de identiteit van verdachten met behulp van de technische voorziening (de ID-zuil), worden de ingevoerde (politie)gegevens vergeleken en gekoppeld met meerdere databronnen. Dit zijn de volgende databanken: HAVANK, VVI en SKDB.

Nu in ieder geval drie van de negen criteria vervuld zijn gaat er van de verwerking Uitvoeren identiteitsonderzoek (1e lijns) een hoog risico voor de rechten en vrijheden van betrokkene uit en is het derhalve noodzakelijk om een GEB uit te voeren op de verwerking.

4. Politiegegevens

Beschrijf per categorie betrokkene de politiegegevens die worden verwerkt. Geef aan of het algemene of bijzondere politiegegevens zijn. Voeg een dataoverzicht van de applicaties toe als bijlage.

4a. Geef een beschrijving van de categorie betrokkenen en de categorie politiegegevens

Categorie betrokkenen	Soort persoonsgegeven	Type
Verdachte	**Biografische gegevens** • Naam, voornaam • Geboortedatum • Geboorteplaats • Nationaliteit • BSN • Adres van inschrijving in BRP • Woon- en verblijfplaats • Zaaknummer • Biometrienummer (HAVANK) • Strafrechtketennummer (SKN)	Politiegegevens
	Biometrische gegevens • Foto gelaat	Bijzondere politiegegevens

[8] Art. 5 Wet politiegegevens.

	• Handpalm • Vingerafdrukken	
Betrokkene in het kader van ID-onderzoeken in het kader van de openbare orde zonder verdenking van een strafbaar feit.	• Naam, voornaam • Geboortedatum • Geboorteplaats • Nationaliteit • BSN • Adres van inschrijving in BRP • Woon- en verblijfplaats • E-mailadres • Telefoonnummer • Strafrechtketennummer (SKN) • Biometrienummer (HAVANK)	Politiegegevens
Politieambtenaar (aanvrager, gebruiker ID-zuil, contactpersoon van een zaak).	**Contactgegevens** • Naam, voornaam • Dienstnummer	Politiegegevens

4b. Wat is de omvang van de gegevensverwerking op jaarbasis en landelijk gezien?
Uit de Veiligheidsmonitor 2023 van het Centraal Bureau voor de Statistiek (CBS) blijkt dat acht procent van de Nederlanders een controle door de politie heeft ervaren. Een onderdeel van een dergelijke controle is veelal een ID-onderzoek. Derhalve is de verwerking als grootschalig aan te merken.

4c. Voeg dataoverzichten per applicatie toe
Het gaat hier om een overzicht van de persoonsgegevens die per systeem, applicatie worden verwerkt.

Data overzicht naam applicatie:
☐ Ja
X Nee

Toelichting:
MEOS Framework - Politie Nederland
BVH - Politie Nederland
5.1.2.i 2.0 - Politie Nederland
Politiekalender – Politie Nederland
Live Journaal Politie – Politie Nederland

5. Gegevensstroom

Beschrijf de gegevensstroom aan de hand van de verschillende stadia van een verwerking. Benoem tevens de middelen en systemen die voor de verwerking gebruikt worden. Wanneer er een gegevensstroomschema of werkprocesbeschrijving beschikbaar is, kun je deze als bijlage toevoegen.

5a. Beschrijf de stadia van de gegevensstroom

Identificatie kan worden uitgevoerd zonder of met gebruikmaking van een foto en vingerafdrukken. Beide procedures worden hieronder in de tabel uitgelegd.
In de tabel wordt gebruik gemaakt van procedures met de codes P1 t/m P5. Hieronder volgt een korte omschrijving wat de procedure inhoudt:

Code	Omschrijving	Doel
P1a	Standaardprocedure identificatie	Doel is identificatie van de identiteit van een verdachte.
P1ab	Standaardprocedure identificatie verdenking van een strafbaar feit	Doel is identificatie van de identiteit van een betrokkene in het kader van de handhaving van de openbare orde zonder
P1b	Standaardprocedure verificatie	Doel is verificatie van de identiteit van een verdachte
P2	Verificatie met vingerafdrukken	Doel is om eenvoudig en snel met gebruikmaking van vingerafdrukken en/of gelaatsfoto's de identiteit van de verdachte vast te stellen of het verifiëren van zijn identiteit.
P3	Identificatie met foto + vingerafdrukken	Doel is om eenvoudig en snel met gebruikmaking van vingerafdrukken en/of gelaatsfoto's de identiteit van de verdachte vast te stellen of het verifiëren van zijn identiteit.
P4	Identificatie met foto + vingerafdrukken	Doel is om eenvoudig en snel met gebruikmaking van vingerafdrukken en/of gelaatsfoto's de identiteit van de verdachte vast te stellen of het verifiëren van zijn identiteit.
P5	Nader identiteitsonderzoek	Doel is om alle twijfels omtrent de identiteit van betrokken weg te nemen met behulp van onderzoek als bedoeld in

5.1.2.i


5.1.2.i

5b. Welke werkprocessen zijn beschikbaar om inzicht te krijgen in de verwerking?
De volgende werkprocessen in de bedrijfsarchitectuur zijn te koppelen aan de verwerking:
Uitvoeren identiteitsonderzoek (1e lijns)

Een of meerdere werkprocessen sluiten niet aan op de verwerking in de praktijk, is/zijn onvolledig, niet meer actueel:
De werkprocessen inclusief bijbehorende verwerking van persoonsgegevens met betrekking tot de ID-onderzoeken 1e lijns in het kader van de openbare orde is niet beschreven in de bedrijfsarchitectuur waardoor er onduidelijkheid bestaat over het juridisch kader hieromtrent.

5c. Overzicht van de gegevensstroom bijgevoegd:
X **Ja, in het geval er tegen de betrokkene een vermoeden bestaat van een strafbaar feit. De gegevensstroom omtrent de controles in het kader van de openbare orde handhaving is hierin niet opgenomen en ook niet aanwezig** (zie bijlage II).
☐ **Nee**

Toelichting:
Bijlage II: Stroomschema ID-vaststelling het betreft alleen het stroomschema verdachte (blauwe lijn).

5d. Eigen beheerde omgeving
Er wordt in het kader van deze verwerking geen gebruik gemaakt van een eigen beheerde omgeving.

6. Doel van de verwerking

Beschrijf het doel van de (voorgenomen) gegevensverwerking en eventuele andere doelen die gerelateerd zijn aan de verwerking. Beschrijf waar de verwerking concreet voor bedoeld is en waar het op gericht is.

Verwerking	Doel van de verwerking
P1 (a+b) Standaardprocedure identificatie	Doel is identificatie en verificatie van de identiteit van een verdachte.
P1ab Standaardprocedure identificatie	Doel is om de identiteit vast te stellen van een betrokkene in het kader van de handhaving van de openbare orde. Bijvoorbeeld om afspraken te maken in het kader van burenruzies, sportwedstrijden of met demonstratieleiders en/of demonstranten.
P2 tot en P4	Doel is om eenvoudig en snel met gebruikmaking van vingerafdrukken en/of gelaatsfoto's de identiteit van de verdachte vast te stellen of het verifiëren van zijn of haar identiteit.
P5	Doel is om alle twijfels omtrent de identiteit van betrokkene weg te nemen met behulp van onderzoek als bedoeld in artikel 61a Sv.

7. Betrokken partijen en hun belangen

Partij	Rol	Politiegegevens
Binnen het politiedomein		
Collega's in de uitvoering van de politietaak.	Raadplegen en muteren van politiegegevens	Politiegegevens en bijzondere politiegegevens
Buiten het politiedomein		
Officier van Justitie	Bevoegd gezag in het kader van strafrechtelijke handhaving. Ontvanger.	Politiegegevens en bijzondere politiegegevens
Ministerie van J&V (Justid)	Verwerkingsverantwoordelijke voor de SKDB. Ontvanger en verstrekker	Politiegegevens en bijzondere politiegegevens

Burgemeester	Bevoegd gezag in het kader van de handhaving van de openbare orde.	Er worden geen gegevens met betrekking tot identiteitsonderzoeken gedeeld met de burgemeester.

8. Autorisaties

Antwoord:

Autorisatieprofielen zijn conform IAM (Identity & Access Management) ingeregeld en worden op basis van de basisfunctie en werkplek van medewerkers toegekend. In de praktijk worden de politiegegevens intern ter beschikking gesteld aan personen die zijn geautoriseerd volgens het autorisatiebeleid voor het verwerken van politiegegevens, tenzij anders is bepaald in de [redacted]. Via [redacted] kunnen daarom aanvullende autorisaties verleend worden die nodig zijn voor de specifieke taak van de medewerker.

Wanneer aanvullende autorisaties nodig zijn, zoals het geval is bij medewerkers met taakaccenten, kan er een aanvraag gedaan worden via [redacted]. Deze aanvraag wordt handmatig getoetst door een leidinggevende en al dan niet toegekend.

Na het verlenen van autorisaties via [redacted] dient periodiek gecontroleerd te worden of de aanvullende autorisaties nog noodzakelijk zijn. Een verleende autorisatie is echter maximaal twee jaar geldig, zonder actief handelen wordt deze automatisch ingetrokken.

Ambtenaren van politie zijn wettelijk bevoegd tot het vaststellen van identiteitsgegevens. Met betrekking tot de ID-zuil hebben alle gebruikers een opleiding gevolgd. Na het volgen van deze opleiding worden zij persoonlijk geautoriseerd voor het gebruiken van de ID-zuil voor alle werkzaamheden, dus ook het nemen van vingerafdrukken en het maken van een gelaatsfoto.

9. Verwerkingslocaties

x Nederland
☐ overige lidstaten binnen de EU namelijk:
☐ doorgifte aan een derde land of internationale organisatie:

Toelichting:
De verwerking van politiegegevens, opslag van gegevens en gebruikte systemen vindt plaats in Nederland.

10. Verwerkingstermijnen

Applicatie:

Het betreft primair een proces conform art. 8 Wpg. De bewaartermijnen vanuit de Wpg zijn uitgewerkt in de registratieve systemen. Eventuele verwijdering en vernietiging vindt plaats in de (registratieve) systemen. Onderstaand zijn de termijnen en werkwijzen beschreven per registratiesysteem.

BVH en Summ-IT: formulieren sets (terugmeldingen vanuit SKDB) kunnen in BVH en Summ-IT worden opgeslagen of toegevoegd worden aan een proces-verbaal. In dat geval gelden de binnen de politie gehanteerde reguliere regels m.b.t. bewaartermijnen en termijnen van verjaring. Er is sprake van een geautomatiseerd proces in beide systemen waardoor er op individueel niveau geen afwijkingen mogelijk zijn.

- Voor BVH geldt een verwerkingstermijn van 5 jaar vanaf de eerste verwerking, waarbij de gegevens na het eerste jaar alleen nog te raadplegen zijn wanneer er gericht gezocht wordt;
- Voor Summ-IT geldt een verwerkingstermijn van 5 jaar vanaf de eerste verwerking van politiegegevens die vallen onder artikel 8 Wpg.

SKDB: het beheer van de SKDB is door de minister van Justitie en Veiligheid belegd bij Justitiële Informatiedienst, afdeling Matching (de Matching Autoriteit). Zij zijn wettelijk gezien de verwerkingsverantwoordelijke voor de databank en daarmee zelfstandig verantwoordelijk voor het hanteren van de juiste bewaar- en vernietigingstermijnen. Aangezien de SKDB niet onder de verwerkingsverantwoordelijkheid van de politie valt is het bepalen en beoordelen van de verwerkingstermijnen van de SKDB niet in scope van deze GEB. Wel valt op te merken dat het verwijderingsproces

voor de betrokkene ingewikkeld kan zijn als achteraf blijkt dat de politie iemand ten onrechte in het SKDB heeft opgenomen, deze zouden dan ook niet meer (verder) verwerkt moeten worden.

De systemen die geraadpleegd worden in het kader van deze verwerking, 5.1.2.I en MEOS, maken gebruik van de gegevens van bovengenoemde systemen (BVH en Summ-IT). Logging en monitoring van raadplegingen wordt door de politie vastgelegd ten behoeve van de waarheidsvinding en voor integriteitsonderzoeken conform art. 32a Wpg.

Op dit moment vindt er door een besluit van de korpschef (met goedkeuring van de minister van Justitie en Veiligheid) in geen van de systemen vernietiging plaats. De gegevens kunnen wel op verzoek van betrokkene (art. 28 Wpg), en na toetsing door politie, ambtshalve door de Poortwachter in voorkomende gevallen verwijderd worden.

Politiekalender: De politiekalender is een landelijke applicatie voor het registreren van evenementen en (risicovolle) gebeurtenissen. Dit biedt de basisteams, districten, eenheden inzicht in de evenementen en de bijbehorende inzet. Een demonstratie is een voorbeeld van een evenement die in de politiekalender wordt opgenomen. Er worden, indien er sprake is van een aangemelde demonstratie, persoonsgegeven van de aanmelder verwerkt. Deze zouden verwerkt moeten worden conform art. 8 Wpg, onduidelijk is of deze termijnen ook worden nageleefd.

Live Journaal Politie: Live Journaal Politie wordt gebruikt om werkinhoudelijke informatie uit te wisselen tussen collega's. In het kader van de inzet tijdens een demonstratie zouden mogelijk identiteiten van demonstranten verder worden verwerkt.

11. Juridisch en beleidsmatig kader

Benoem de wet- en regelgeving en beleid die een rol spelen voor de (voorgenomen) gegevensverwerking. De Wpg kan hier weggelaten worden tenzij er een bijzondere situatie aan de orde is.

Juridisch en/of beleidsmatig kader	Wetsartikelen en toelichting
Juridisch kader	
Grondwet	In artikel 10 van de Grondwet is opgenomen dat iedereen recht heeft op eerbiediging van zijn of haar persoonlijke levenssfeer. De wet kan in bepaalde gevallen dit recht beperken, bijvoorbeeld bij de opsporing van misdaden.
Europees Verdrag voor de Rechten van de Mens	Artikel 8 EVRM omvat o.a. het recht op privéleven. De wet kan in bepaalde gevallen dit recht beperken, bijvoorbeeld bij de opsporing van misdaden.
Wetboek van Strafrecht	Artikel 447e heeft betrekking op de verplichting tot inzage bieden van het identiteitsbewijs.
Wetboek van Strafvordering	Artikel 27a,55c, 61a, 67 lid 1 zijn van toepassing bij het vaststellen van de identiteit.
Politiewet 2012	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. Art. 8 biedt de grondslag voor het controleren van identiteiten.
Wet op de identificatieplicht	In artikel 2 is de toonplicht aan een opsporingsambtenaar vastgelegd.
Besluit identiteitsvaststelling verdachten en veroordeelden	Artikel 2 t/m 10 gaan over de strafrechtsketendatabank en de databank met vingerafdrukken.
Beleidsmatig kader	
Privacybeleid	In het algemene Privacybeleid van de politie zijn de wettelijke verplichtingen uitgewerkt in normen voor de organisatie.
Beleid bewaartermijnen	Het beleid bewaartermijnen geeft de kaders voor de bewaartermijnen binnen de politie.
Handleiding 'Rechten van de betrokkene'	Stappenplan voor de afhandeling van inzage en wijzigingsverzoeken van persoons- en politiegegevens.
Protocol identiteitsvaststelling strafketen 2020	Dit bevat het protocol hoe er om wordt gegaan met identiteitsvaststelling binnen de gehele strafketen. Zie ook de bijlage.

12. Rechten van betrokkenen

Uitvoering rechten betrokkene	Ja	Nee	Toelichting
De portefeuille beschikt over een landelijk protocol om een verzoek voor rechten betrokkene uniform te behandelen, voor de verwerkingen die onder diens verantwoordelijkheid vallen.	X		Er bestaat een landelijke handleiding 'Rechten van Betrokkene'.
De verwerkingsverantwoordelijke heeft een ingericht proces dat aansluit op de Privacydesk.	X		Er is een ingericht proces om de rechten van een betrokkene uit te oefenen.
De systemen zijn in staat om bijv. data te verwijderen of inzage te verlenen.	X		Niet iedere medewerker is geautoriseerd om data te verwijderen of inzage te verlenen.

Toelichting:
Bij de Privacydesk kunnen betrokkenen terecht om een beroep te doen op hun 'rechten van betrokkene'. Politiemedewerkers verwijzen betrokkene door naar de Privacydesk, omdat zij hieraan zelf geen invulling geven. De Privacydesk zal zich, indien nodig wenden tot de betreffende afdeling om de benodigde informatie op te halen. Over deze werkwijze zijn onderling geen schriftelijke werkafspraken gemaakt.

Behandelen verzoeken tot inzage, correctie etc.: Betrokkenen die menen onjuist of ten onrechte geregistreerd te staan in de SKDB (al dan niet als gevolg van identiteitsfraude), kunnen zich wenden tot de minister van Justitie en Veiligheid met een verzoek om inzage dan wel correctie van geregistreerde gegevens (art. 18 Wjsg). De Matching Autoriteit (MA) behandelt namens de minister deze verzoeken. Betreft het verzoek of de klacht een bestand dat niet door de MA wordt beheerd, dan wordt de klacht doorgezonden naar de verantwoordelijke voor het desbetreffende bestand. De MA draagt naar vermogen bij aan een praktische en effectieve oplossing. Voor zover mogelijk worden verzoeken informeel afgehandeld. Wijzigingen in vastgelegde gegevens worden gelogd. Als de betrokkene de politie vraagt hoe hij of zij de rechten kunnen uitoefenen zal de politie de betrokkene verwijzen naar Justid.

B. Beoordeling rechtmatigheid gegevensverwerking

13. Wettelijke doeleinden

Bepaal op welke wettelijke doeleinden (politietaken) de gegevensverwerking is gericht en motiveer waarom deze verwerking onder de gekozen wettelijke doeleinde valt. Deze doeleinden moeten aan wettelijke voorwaarden voldoen, beoordeel hoe aan deze voorwaarden wordt voldaan.

De wettelijke doeleinden zijn:

- Artikel 8 Wpg (uitvoering van de dagelijkse politietaak)
- Artikel 9 Wpg (onderzoek i.v.m. de handhaving van de rechtsorde in een bepaald geval)
- Artikel 10 Wpg (inzicht betrokkenheid van personen bij:
  - a) het beramen of plegen van misdrijven;
  - b) bepaalde ernstige bedreigingen van de rechtsorde;
  - c) ernstige schending van de openbare orde.)
- Artikel 12 Wpg (informanten)
- Artikel 13 Wpg (ondersteunende taken, schriftelijke vastlegging vereist)
- Artikel 22 Wpg (wetenschappelijk onderzoek en statistiek)

Wettelijke doeleinden	Toetsing
Artikel 8 Wpg	Het vaststellen van de identiteit is op grond van artikel 3 Politiewet 2012 een dagelijkse politietaak. Iedere opsporingsambtenaar is daartoe bevoegd o.g.v. artikel 8 Politiewet. Iedere opsporingsambtenaar is tevens bevoegd tot het bedienen van de ID-zuil na het volgen van een hierop gerichte opleiding. Er is voor wat betreft de verwerkingsgrondslag geen verschil tussen een ID-onderzoek in de strafrechtketen of een onderzoek in het kader van de openbare orde handhaving.
Artikel 13 lid 1 sub c Wpg	Identificatie van personen of zaken: het doel van het vaststellen of verifiëren van ID of toekennen SKN indien dit het eerste strafbare feit is. Er is geen sprake van schriftelijke vastlegging conform art. 13 lid 4 Wpg en art. 6:2 Bpg.

14. Bijzondere politiegegevens

In deel A is beschreven of en welke bijzondere politiegegevens worden verwerkt. Het verwerken van bijzondere politiegegevens gebeurt uitsluitend als dit onvermijdelijk is voor het doel van de verwerking, een aanvulling is op de verwerking van andere politiegegevens betreffende de persoon en de gegevens afdoende zijn beveiligd, art. 5 Wpg.

Beoordeel of de verwerkte bijzondere politiegegevens voldoen aan de vereisten van artikel 5 Wpg:

Wettelijke eis	Toetsing
De aangegeven te verwerken bijzondere politiegegevens zijn onvermijdelijk en een aanvulling op de verwerking	Voor de verwerking van bijzondere politiegegevens geldt dat deze alleen plaats mogen vinden wanneer dit onvermijdelijk is voor het doel van de verwerking en in aanvulling zijn op de verwerking van andere politiegegevens. Bij deze verwerking worden enkel bijzondere politiegegevens verwerkt die onvermijdelijk zijn om tot het doel van de verwerking te komen, namelijk identiteitsvaststelling. Dit geldt zowel voor de vergelijking van de pasfoto op een identiteitsbewijs als voor het afnemen van een gelaatsfoto en/of vingerafdrukken bij de ID-zuil.
De te verwerken bijzondere politiegegevens zijn afdoende beveiligd	Elke politieambtenaar heeft een eigen inlogcode. De database beveiliging ligt bij de beheerder de database (Justid).

15. Verdere verwerkingen

Alle verwerkingen vinden plaats binnen Nederland op een politielocatie.

Beoordeel in geval van een verdere verwerking of aan de wettelijke vereisten is voldaan:

Verdere verwerkingen	Toetsing
Op basis van artikel 8, derde, vierde lid Wpg	Politiegegevens, die worden verwerkt op grond van het eerste, tweede en derde lid, kunnen ter beschikking worden gesteld voor verdere verwerking op grond van de artikelen 9, 10 en 12 Wpg. In dit geval is er geen sprake van verdere verwerking want bij deze verwerking betreft het een eerste contact moment. De gegevens die hierbij worden verwerkt kunnen mogelijk later wel door de politie verder worden verwerkt in het kader van een andere verwerking, maar dat is buiten scope van deze GEB.
Artikel 13 lid 1 en 2 Wpg	Politiegegevens kunnen ter ondersteuning van de politietaak verder worden verwerkt voor bepaalde doeleinden beschreven in artikel 13 Wpg. De verwerking dient dan echter wel vastgelegd te worden in een artikel 13 protocol.

16. Autorisaties

Iedere verwerking van politiegegevens dient te voldoen aan het systeem van autorisaties zoals bedoeld in artikel 6. De terbeschikkingstelling van politiegegevens hangt samen met de autorisaties.

Beoordeel of de verwerking voldoet aan de voorwaarden van autorisaties
Meerdere antwoorden zijn mogelijk zo nodig per systeem beoordelen.

Antwoord:
Bij deze verwerking zijn meerdere afzonderlijke applicaties betrokken. Iedere applicatie kan de autorisatie op een andere manier hebben geregeld. Of de autorisatie van een specifieke applicatie voldoet aan de gestelde eisen wordt bepaald door het uitvoeren van een aantal vragenlijsten, waaronder de BIO-QuickScan. Indien de autorisatie van een applicatie niet voldoet óf als niet duidelijk is hoe de autorisaties is geregeld, zal dit opgenomen worden in onderdeel 'risico's en maatregelen'.

Autorisatieprofielen zijn conform IAM (Identity & Access Management) ingeregeld en worden op basis van de basisfunctie en werkplek van medewerkers toegekend. In praktijk worden de politiegegevens intern ter beschikking gesteld aan personen die zijn geautoriseerd volgens het autorisatiebeleid voor het verwerken van politiegegevens, tenzij anders is bepaald in [redacted]. Via [redacted] kunnen daarom aanvullende autorisaties verleend worden die nodig zijn voor de specifieke taak van de medewerker.

Wanneer aanvullende autorisaties nodig zijn, zoals het geval is bij medewerkers met het taakaccenten, kan er een aanvraag gedaan worden via [redacted]. Deze aanvraag wordt handmatig getoetst door een leidinggevende en al dan niet toegekend.

Na het verlenen van autorisaties via [redacted] dient periodiek (dus binnen de termijn van twee jaar waarin de autorisatie sowieso dient te worden) gecontroleerd te worden of de aanvullende autorisaties nog noodzakelijk zijn. Uit het onderzoek in het kader van deze GEB blijkt echter dat dit niet altijd periodiek gecontroleerd wordt. [redacted] Daarnaast is het belangrijk om autorisaties om ID-onderzoeken uit te voeren zo snel mogelijk worden ingetrokken als collega's een andere werkplek in/extern hebben verkregen waarbij de autorisaties niet meer nodig zijn. Indien de collega intern een nieuwe functie krijgt dient altijd opnieuw bekeken te worden welke autorisaties hierbij horen.

17. Verstrekkingen aan externe partijen

De Wpg kent een gesloten stelsel voor de verstrekkingen aan partijen buiten het politiedomein. Per externe partij moet de verstrekking worden beoordeeld op wettelijke grondslag en proportionaliteit en subsidiariteit.

Beoordeel of de verstrekkingen aan externe partijen voldoen aan de wettelijke vereisten.

- Verstrekking aan gezagsdragers: artikel 16 Wpg
- Verstrekking aan inlichtingendiensten: artikel 17 Wpg
- Verstrekking aan derden structureel: artikel 18 Wpg
- Verstrekking aan derden incidenteel: artikel 19 Wpg
- Verstrekking aan derden structureel voor een samenwerkingsverband: artikel 20 Wpg
- Rechtstreekse verstrekking: artikel 23 Wpg
- Rechtstreekse verstrekking aan inlichtingen- en veiligheidsdiensten: artikel 24 Wpg

Politiegegevens over de identiteit van de verdachte worden geüpload naar de SKDB voor het aanmaken van een SKN. De verzamelde documenten als scan paspoort, vingerafdrukken of gelaatsfoto worden niet verstrekt aan derden als bedoeld in de bovenstaande artikelen.

18. Doorgifte aan derde landen

Beoordeel of de doorgifte van politiegegevens aan derde landen voldoet aan artikel 15a en 17a Wpg.

Alle verwerkingen vinden plaats binnen Nederland op een politielocatie. Wel kunnen er politiegegevens doorgegeven worden aan derde landen of Interpol i.v.m. het vaststellen van de identiteit van een verdachte. Dit kan ook met de databanken waar de gelaatsfoto en vingerafdrukken in worden opgeslagen.

Naam derde landen	Toetsing doorgifte
Lidstaten Europese Unie	Art. 15a Wpg regelt de ter beschikkingstelling van politiegegevens aan instanties die belast zijn met de politietaak binnen de lidstaten van de Europese Unie. In art. 5:5 Bpg is een bepaling opgenomen die specifiek ziet op de geautomatiseerde doorzending van dactyloscopische gegevens. Art. 15a lid 1 Wpg vereist voor de ter beschikkingstelling van politiegegevens dat er een rechtsinstrument op grond van het VwEU aan ten grondslag ligt. Het Prüm-besluit beantwoordt aan deze eis. Ter beschikkingstelling van politiegegevens vindt plaats conform de in art. 15a Wpg en art. 5:5 Bpg beschreven procedures. De ter beschikkingstelling van de HAVANK-strafrechtdatabase ten behoeve van geautomatiseerde doorzoeking voldoet aan de criteria van art. 15a Wpg.

Meer informatie over de biometrische gegevens (gelaatsfoto en vingerafdrukken) is te vinden in het addendum op de GEB HAVANK 4 en CATCH 2 m.b.t. Dactyloscopie en het addendum op de GEB Biometrievoorziening HAVANK 4 & CATCH 2 m.b.t. Gelaatsvergelijking.

19. Noodzakelijkheid, rechtmatigheid en doelbinding

Politiegegevens worden slechts verwerkt als dit noodzakelijk is voor de wettelijke doeleinden, behoorlijk en rechtmatig is, de gegevens rechtmatig zijn verkregen, gelet op de doeleinden toereikend, ter zake dienend en niet bovenmatig zijn, artikel 3 lid 1 en 2 Wpg.

19a. Beoordeel of de verwerking en de verdere verwerkingen zoals terbeschikkingstellingen en verstrekkingen voldoen aan de criteria van noodzakelijkheid, rechtmatigheid en doelbinding.

Criteria	Verwerking	Verdere verwerking
Proportionaliteit *Staat het belang van de verwerking in verhouding tot de beperking van de persoonlijke levenssfeer?*	Uitvoeren identiteitsonderzoek 1e lijns	Het is niet mogelijk om met de inzet van andere (minder ingrijpende) middelen hetzelfde doel te behalen. Bij een identiteitscontrole worden de middelen steeds ingrijpender, afhankelijk van de situatie. Van het vergelijken van de foto om de identiteit vast te stellen tot aan het afnemen van vingerafdrukken. Tijdens de verwerking worden algemene en bijzondere politiegegevens verwerkt. De gegevensverwerking is noodzakelijk om het beoogde doel te bereiken (het vaststellen van de identiteit) en staat in verhouding tot de inbreuk op de privacy. Het kan namelijk nodig zijn om biometrie of pasfoto's te gebruiken om daadwerkelijk vast te stellen wie de betrokkene is. Uit de gesprekken is gebleken dat de gegevens die gemuteerd worden zorgvuldig zijn afgewogen door de medewerker op noodzakelijkheid. Binnen deze verwerking vindt indien nodig een integrale bevraging van politiesystemen plaats. Deze informatie is noodzakelijk voor het doel omdat enkel met de juiste gegevens de identiteit vastgesteld kan worden van de verdachte.
Proportionaliteit t.a.v. identiteitsonderzoeken in het kader van de openbare orde zonder verdenking van een strafbaar feit. *Staat het belang van de verwerking in verhouding tot de beperking van de persoonlijke levenssfeer?*	Uitvoeren identiteitsonderzoek 1e lijns	Voor wat betreft de handelingen en raadplegingen tijdens identiteits-onderzoeken in het kader van de openbare orde is de verwerking t.a.v. de proportionaliteit niet anders dan het reguliere proces t.a.v. de verdachte waarvan een verdenking van een strafbaar feit bestaat. Gezien het fundamentele belang van het demonstratierecht voor de democratische rechtsorde en het feit dat politieoptreden een verlammend effect kan hebben is het van belang dat de politie in dit verband extra kritisch omgaat met haar bevoegdheden en dus met gepaste terughoudend omgaat met het verrichten van identiteitsonderzoeken op basis van art. 3 en 8 Pw 2012. Doordat er voor operationele collega's geen handelings- of inzetkader voor collega's in de operatie beschikbaar is kan het zijn dat er meer identiteitsonderzoeken plaatsvinden dan strikt noodzakelijk voor de uitvoering van de politietaak, hetgeen de proportionaliteit van de verwerking raakt.
Subsidiariteit *Zijn andere minder in de persoonlijke levenssfeer van de burger ingrijpende maatregelen mogelijk?*	Uitvoeren identiteitsonderzoek 1e lijns	Het is niet mogelijk de politiegegevens op een voor de betrokkene minder nadelige en ingrijpende wijze te verwerken, omdat de gegevens die verwerkt worden noodzakelijk zijn om de juiste inzet en routering te bepalen.

Niet bovenmatig *Is de verwerking niet bovenmatig en niet meer dan nodig voor het doel?*	Uitvoeren identiteitsonderzoek 1e lijns	Vanuit het onderzoek en de gesprekken blijkt dat voor wat betreft het verwerkingsdoeleinde enkel de noodzakelijke gegevens die benodigd zijn voor de identiteitscontrole worden gemuteerd. De integrale bevraging draagt daarnaast bij aan het doel van de verwerking en het bepalen van de juiste vervolgaanpak. Wel dient actief gecontroleerd te worden of de bevraagde registers noodzakelijk zijn voor het ID-onderzoek.

19b. Beoordeel of de gegevens rechtmatig zijn verkregen

Rechtmatige verkrijging	Toetsing
Rechtmatigheid verkrijging	Tijdens een identiteitscontrole is de informatie, behoudens het oneigenlijk gebruik van systemen, rechtmatig verkregen.

20. De verwerker

De politie kan een verwerker inschakelen om politiegegevens onder het gezag van de politie te verwerken (artikel 6c Wpg).

In het kader van deze verwerking wordt geen gebruik gemaakt van een verwerker.

21. Beoordeling verwerkingstermijnen

In beginsel wordt een identiteitsonderzoek niet gemuteerd in bijv. BVH. De bevragingen worden wel opgenomen in de logging van de (politie)systemen die bevraagd worden. Indien de identiteit van een verdachte is vastgesteld worden de gegevens opgeslagen in de SKDB en gelden daarvoor de reguliere bewaartermijnen uit de wet politiegegevens niet omdat Justid (Ministerie J&V) de dienst faciliteert voor de gehele strafrechtketen en de politie daar geen verwerkingsverantwoordelijkheid over draagt. De verwerkingstermijnen, voor wat betreft de logging in politiesystemen, is conform art. 8 Wpg.

21b. Beantwoord deze vraag in het geval er sprake is van een verwerking voor ondersteunende taken, artikel 13 verwerking.

Antwoord:
Ten behoeve van de ondersteuning van de politietaak kunnen de politiegegevens die worden verwerkt overeenkomstig artikel 8, 9 en 10, verder worden verwerkt voor zover zij relevant zijn voor: identificatie van personen of zaken (artikel 13 li 1 sub c Wpg)

22. Rechten van betrokkenen

Uitvoering rechten betrokkene	Beoordeling
Recht op informatie (artikel 24a en 24b Wpg)	Er staat een Privacyverklaring op politie.nl. Er wordt niet actief op de privacyverklaring gewezen bij contact met de politie, echter kan aan deze informatieplicht op algemene wijze worden voldaan.
Recht op inzage (artikel 25 lid 1 Wpg)	De betrokkene kan schriftelijk een inzageverzoek indienen bij de Privacydesk. De Privacydesk voert daarna een zoekslag uit in de systemen en contacteert de relevante gebruikers van de betreffende systemen in de eenheden om de informatie te ontvangen die over de betrokkene verwerkt wordt.
Recht op rectificatie (artikel 28 lid 1 Wpg)	De betrokkene kan schriftelijk een rectificatieverzoek indienen bij de Privacydesk. De Privacydesk beoordeelt daarna het verzoek. Wanneer er sprake is van een onjuiste of onvolledige verwerking, neemt de Privacydesk contact op met de gebruikers van het betreffende systeem in de eenheden om

Uitvoering rechten betrokkene	Beoordeling
	de politiegegevens te rectificeren of aanvullen.
Recht op vernietiging (artikel 28 lid 2 Wpg)	De betrokkene kan schriftelijk een vernietigingsverzoek indienen bij de Privacydesk. Dit verzoekt wordt vervolgens beoordeeld door de Privacydesk. Indien de Privacydesk concludeert dat de politiegegevens vernietigd moeten worden, dan wordt een melding gedaan bij de Servicedesk ICT om de registratie ook daadwerkelijk te vernietigen. Dit is in lijn met het Beleid Bewaartermijnen zoals deze binnen de politie gehanteerd wordt.

Betrokkenen die menen onjuist of ten onrechte geregistreerd te staan in de SKDB (al dan niet als gevolg van identiteitsfraude), kunnen zich wenden tot de minister van Justitie en Veiligheid met een verzoek om inzage dan wel correctie van geregistreerde gegevens (art. 18 Wjsg). De MA behandelt namens de minister deze verzoeken. Betreft het verzoek of de klacht een bestand dat niet door de MA wordt beheerd, dan zet zij de klacht door naar de verantwoordelijke voor het desbetreffende bestand. De MA draagt naar vermogen bij aan een praktische en effectieve oplossing van het gerezen probleem. Voor zover mogelijk worden verzoeken informeel afgehandeld. Wijzigingen in vastgelegde gegevens worden gelogd.[9]

[9] Hoewel het proces rondom de rechten van betrokkenen van de SKDB buiten de scope van deze GEB valt dient de politie de betrokkene hierin wel adequaat te faciliteren en te informeren, derhalve is dit proces toch opgenomen. Zie ook: Borst, W. (2019). De verdachte in de ketens. Boom bestuurskunde p.3.6 en 3.8.

C. Beschrijving en beoordeling risico's en maatregelen

Beschrijf en beoordeel de risico's van de (voorgenomen) gegevensverwerkingen voor de rechten en vrijheden van de betrokkenen.

De privacy risicoanalyse Wpg

De privacy risicoanalyse is gebaseerd op het model DPIA rijksdienst 2021. Het formulier maakt onderdeel uit van het format GEB-formulier Wpg maar kan ook als zelfstandig formulier worden gebruikt. Het gaat bij privacy risico's primair om de gevolgen voor de betrokkene. Naast de risico's voor de betrokkene bestaan er ook risico's voor de organisatie. Voor de inschatting van de risico's wordt onderstaande risicomatrix, waarderingstabel toegepast. Het tweede deel bestaat uit de geadviseerde maatregelen en een inschatting van het restrisico voor en na het nemen van mitigerende maatregelen. De risico's en maatregelen zijn in overeenstemming met de Wpg bijv. met betrekking tot de doelen van de verwerking en de verwerking van bijzondere gegevens. Onder gegevens wordt verstaan politiegegevens in de zin van artikel 1 Wpg.

Risico´s en maatregelen

Beschrijf en beoordeel de risico's van de gegevensverwerkingen voor de rechten en vrijheden van betrokkenen. Secundair gaat het om de risico's voor de organisatie. Ga hierbij in ieder geval in op welke negatieve gevolgen de gegevensverwerkingen kunnen hebben voor:

- De rechten en vrijheden van de betrokkenen, zoals het verbod op discriminatie;
- De oorsprong van deze gevolgen;
- De waarschijnlijkheid (kans) dat deze gevolgen zullen intreden;
- De ernst (impact) van deze gevolgen voor de betrokkenen wanneer deze intreden.

Risicomatrix verwerkingen Wpg

		Impact				
		1. Verwaarloosbaar	**2. Minimaal**	**3. Gemiddeld**	**4. hoog**	**5. Kritisch**
Kans	**5. Zeer groot**	**5** GEMIDDELD	**10** GEMIDDELD	**15** HOOG	**20** KRITISCH	**25** KRITISCH
	4. Groot	**4** GEMIDDELD	**8** GEMIDDELD	**12** HOOG	**16** HOOG	**20** KRITISCH
	3. Gemiddeld	**3** LAAG	**6** GEMIDDELD	**9** GEMIDDELD	**12** HOOG	**15** HOOG
	2. Klein	**2** LAAG	**4** LAAG	**6** GEMIDDELD	**8** GEMIDDELD	**10** GEMIDDELD
	1. Zeer klein	**1** VERWAARLOS-BAAR	**2** LAAG	**3** LAAG	**4** GEMIDDELD	**5** GEMIDDELD

		Impact				
		1. Verwaarloosbaar	**2. Minimaal**	**3. Gemiddeld**	**4. hoog**	**5. Kritisch**
	Privacy	Zeer weinig impact voor de betrokkene.	Beperkte impact voor de betrokkene betreffende **algemene** politiegegevens.	Gemiddelde impact voor de betrokkene betreffende **algemene politiegegevens en/of te relateren aan een overtreding.**	Ernstige impact voor de betrokkene betreffende **algemene** politiegegevens en **bijzondere** politiegegevens of **politiegegevens te relateren aan een misdrijf.**	Ernstige impact voor wat betreft de rechten van betrokkenen betreffende **algemene** politiegegevens en **bijzondere** politiegegevens of politiegegevens te relateren aan een **ernstig misdrijf.**

Privacy Risico Analyse Wpg inclusief maatregelen en restrisico's

Categorieën	Geconstateerde privacy issues /risico's	Kans	Impact	Inschatting	Maatregelen Standaard	Kans	Impact	Restrisico
1. Organisatie								
Transparantie	**Issue** Er is geen art. 13 protocol voor de applicatie HAVANK waardoor de verwerking niet transparant is. **Risico**: Hierdoor is de verwerking niet conform wet- en regelgeving en loopt de betrokkene het risico dat o.a. er teveel gegevens worden verwerkt, dreigt voor de organisatie stopzetten van de verwerking, een boete en imagoschade.	5	3	15	Stel een art. 13 Wpg protocol op voor de verwerking van gegevens binnen HAVANK.	1	1	1
Autorisaties	**Issue**: Autorisaties die verleend zijn via 5.1.2.I worden niet altijd periodiek gecontroleerd. **Risico**: 5.1.2.I	3	3	9	Controleer de autorisaties periodiek en borg dit binnen de werkprocessen om te voorkomen 5.1.2.I	1	2	2
Werkwijze ID-controle binnen openbare orde.	**Issue:** Er is geen vastgesteld werkproces en/of protocol om ID-onderzoeken uit te voeren indien dit specifiek gaat om de handhaving van de openbare orde (voornamelijk in het kader van demonstraties). Derhalve worden de ID-onderzoeken mogelijk niet altijd conform wet- en regelgeving uitgevoerd. **Risico:** (negatieve) gedragsveranderingen van betrokkenen, mogelijk onrechtmatige gegevensverwerking, reputatieschade en boetes.	3	4	12	Stel een werkproces/protocol op zodat in de operatie duidelijkheid bestaat omtrent het juridisch en beleidsmatig kader.	1	2	2
2. Mens								
Kennis	**Issue**: Medewerkers zijn onvoldoende op de hoogte van de privacy aspecten van een ID-onderzoek. Dit is onder andere gebleken in het kader van de ID-controles in het kader van de openbare orde handhaving.	3	3	9	Jaarlijks te houden training toegepast op de operatie.	2	2	4

Categorieën	Geconstateerde privacy issues /risico's	Kans	Impact	Inschatting	Maatregelen Standaard	Kans	Impact	Restrisico
	Risico: datalek, misbruik van data voor andere doeleinden, het stilleggen van verwerkingen en boetes.							
3. Gegevens								
Verwerkings termijnen	**Issue:** Voor een artikel 13 lid 1 Wpg verwerking ontbreekt een schriftelijke vastlegging van de verwerkingstermijn. **Risico:** De duur van de verwerking is hierdoor onvoldoende bepaald, dit kan leiden tot misbruik van gegevens.	5	3	15	Bepaal de verwerkingstermijnen en zorg voor een schriftelijke vastlegging en geef instructies aan de medewerkers om hier uitvoering aan te geven.	1	1	1
Verwerkings termijnen	**Issue:** Onduidelijk is of de verwerkingstermijnen in de politiekalender worden nageleefd. Risico: De duur van de verwerking is te lang waardoor er sprake kan zijn van een onrechtmatige gegevensverwerking	5	2	10	Richt de bewaartermijnen in conform art. 8 en leef deze na.	1	1	1
(Rechten van betrokkenen) Verwijderen en vernietigen	**Issue:** Indien blijkt dat iemand door de politie ten onrechte is opgenomen in de SKDB is het verwijderingsproces ingewikkeld voor de betrokkene. De politie zou hierin beter kunnen ondersteunen. **Risico:** De rechten van betrokkenen (weliswaar ten aanzien van verwerkingsverantwoordelijke J&V) kunnen mogelijk niet worden uitgeoefend.	2	5	10	Ondersteun de betrokkenen bij het verzoek tot verwijdering uit de SKDB.	1	1	1
4. Technische aspecten	n.v.t.							
5. Externe partijen	n.v.t.							

D. Maatregelen en restrisico´s

In bovenstaande tabel is onderdeel D verwerkt. Er worden mitgerende maatregelen voorgesteld en de classificatie van het restriscio na het treffen van de maatregel wordt weergegeven. Risico's volledig reduceren is (vaak) niet mogelijk. Dit betekent dat er vrijwel altijd een resterend risico zal overblijven. De verwerkingsverantwoordelijke dient te beschrijven hoe het tot dit restrisico is gekomen en waarom deze aanvaardbaar wordt geacht.

Maatregelen
Een passend beveiligingsniveau veronderstelt dat gewerkt wordt met een planning- en controlcyclus (plan-do-check-act) aan de hand waarvan kan worden beoordeeld of de beveiliging steeds adequaat is voor de huidige stand van de techniek en de organisatie.
Voor te treffen maatregelen kan worden aangehaakt bij beveiligingskaders en -standaarden, beste praktijken en goedgekeurde gedragscodes en certificeringsmechanismes. Wanneer een of meerdere van toepassing zijn op de gegevensverwerkingen, beschrijf dan specifiek welke beveiligingsstandaarden, praktijken, gedragscodes en/of certificeringsmechanismes van toepassing zijn en op welke manier deze in de praktijk van toepassing zijn op de gegevensverwerkingen. Bij het bepalen van de gepaste maatregelen moet ook rekening gehouden worden met maatregelen die voortvloeien uit de Baseline Informatiebeveiliging Overheid (BIO).

E. Bijlagen

Bijlage I

5.1.2.i

Bijlage II

Ministerie van Justitie en Veiligheid

Protocol Identiteitsvaststelling strafrechtsketen 2020

Datum 15 april 2021
Status Definitief

Colofon

Afzendgegevens	**Directoraat-Generaal Rechtspleging en Rechtshandhaving** Turfmarkt 147 2511 DP Den Haag Postbus 20301 2500 EH Den Haag www.rijksoverheid.nl/jenv
Auteurs	directoraat-generaal Rechtspleging en Rechtshandhaving

Inhoud

1 Inleiding

1.1 Status en beheer van dit protocol

Status en beheer
Dit protocol hoort bij de Wet identiteitsvaststelling verdachten, veroordeelden en getuigen (hierna: Wivvg; Stb. 2009, 317) en geeft een nadere invulling daaraan. Dit protocol is op 15 april 2021 vastgesteld door de minister van Justitie en Veiligheid, namens deze getekend door de directeur-generaal Rechtspleging en Rechtshandhaving. Het Directoraat-Generaal Rechtspleging en Rechtshandhaving van het Ministerie van Justitie en Veiligheid (DGRR) draagt zorg voor het beheer ervan.

Het protocol heeft het karakter van een in 2006 gemaakte afspraak tussen de in de toenmalige Coördinatiegroep Informatievoorziening Strafrechtsketen (CIS) vertegenwoordigde organisaties over de wijze waarop de wet wordt toegepast.[1] De Rechtspraak en het Openbaar Ministerie nemen daarbij in zoverre een bijzondere plaats in, dat (a) de wet aan rechters en OvJ's geen verplichtingen maar alleen bevoegdheden toekent ten aanzien van de identiteitsvaststelling en (b) die bevoegdheden niet alleen de identiteitsvaststelling van verdachten en veroordeelden betreffen maar ook de identiteitsvaststelling van getuigen. Alles wat in dit Protocol voorgeschreven wordt, moet daarom voor zover het de Rechtspraak en het OM betreft met inachtneming van die bijzondere positie worden gelezen.

Evaluatie van het protocol
Het protocol wordt periodiek, doch in ieder geval om de drie jaar, geëvalueerd en, indien nodig, geactualiseerd. Voorstellen tot wijziging kunnen door de ketenpartners worden ingebracht. Deze zullen worden meegenomen in de periodieke evaluatie- en actualisatieprocedure, of eerder indien noodzakelijk. Alle wijzigingen worden in de vorm van een wijzigingsvoorstel ter beoordeling en goedkeuring voorgelegd aan de Werkgroep Beheer Protocol.[2]

Naleving
De betrokken uitvoerende organisaties zijn zelf verantwoordelijk voor de naleving van de wet en dit protocol. In de praktijk betekent dit dat elke uitvoerende ketenpartner die bij het identificatie- dan wel verificatieproces betrokken is binnen haar organisatie een verantwoordelijke benoemt die toeziet op naleving en juiste toepassing van het protocol, en zo nodig interne maatregelen treft die normconform gedrag bevorderen. Daarnaast wordt periodiek in opdracht van de minister van Justitie en Veiligheid namens deze de directeur-generaal Rechtspleging en Rechtshandhaving een nader in te vullen ketenbrede audit uitgevoerd teneinde na te gaan of het protocol door alle partijen op een juiste wijze wordt toegepast

[1] Op 15 augustus 2017 is het besluit tot instelling van de CIS ingetrokken, Stcrt., 30 augustus 2017, nr. 48944
[2] De werkgroep Beheer Protocol bestaat o.a. uit vertegenwoordigers van politie, KMar, OM, Justid en DGRR.

.

1.2 Doel en achtergrond van het Protocol

In de strafrechtsketen is een deugdelijke vaststelling van de identiteit van personen van fundamenteel belang. Persoonsverwisseling en identiteitsfraude hebben ernstige gevolgen voor de integriteit en effectiviteit van de strafrechtspleging en voor de eventuele slachtoffers van identiteitsfraude. Het is daarom van belang dat de voorgeschreven werkwijze voor het vaststellen van de identiteit van verdachten en veroordeelden aan hoge eisen voldoet en door heel de keten heen eenduidig wordt gevolgd.

Doel van de wet en het protocol is daarom dat op een aantal momenten in een strafrechtelijk traject waarop contact is met een verdachte of veroordeelde diens identiteit met bijzondere zorgvuldigheid wordt vastgesteld. Dit betreft de volgende momenten:

- de aanhouding en voorgeleiding van een verdachte,
- het verhoor van de verdachte door een opsporingsambtenaar, een officier van justitie, de rechter-commissaris of de Raadkamer
- het onderzoek op de terechtzitting,
- de afname van celmateriaal ten behoeve van de bepaling van een DNA profiel,
- de insluiting in een Penitentiaire (of Justitiële jeugd- of GGZ-) Inrichting in het kader van voorlopige hechtenis of de tenuitvoerlegging van een straf of maatregel, en het verlaten van zo'n inrichting,
- contacten met de (jeugd-)reclassering en/of de Raad voor de kinderbescherming en/of een instelling voor GGZ in het kader van advies, reclasseringstoezicht, begeleiding/behandeling en/of werkstraf/taakstraf.

Voor andere categorieën dan de verdachte of veroordeelde, zoals getuigen (in strafzaken) en opgeëiste personen (in uitleveringszaken), betreft de identiteitsvaststelling ingevolge de wet alleen die gevallen dat de rechter twijfelt over de identiteit van betrokkene.

Er zijn onder de huidige wetgeving vier "standaard"-middelen om de identiteit van een verdachte of veroordeelde vast te stellen:

1. de eigen opgave van de betrokkene,
2. een echt, eigen, geldig en gekwalificeerd ID-bewijs ingevolge de Wet op de identificatieplicht,[3]
3. een foto van het gelaat,
4. vingerafdrukken.

De wet geeft aan *welk* middel *wanneer* mag worden ingezet, *wat* de voorwaarden zijn en *welke* functionaris bevoegd is. Als deze middelen geen uitkomst bieden, kunnen alle andere wettige opsporings- en bewijsmiddelen worden ingezet.
Het protocol omschrijft nader *hoe* deze middelen worden toegepast. Het beschrijft op basis van de Wivvg de procedure op hoofdlijnen en de functionele eisen waaraan de vaststelling van de identiteit van verdachten, veroordeelden en getuigen in de strafrechtsketen (en de opgeëiste persoon in uitleveringszaken) moet voldoen. Deze eisen worden nader uitgewerkt in ketenprocesmodellen en vervolgens in de werkprocessen van de ketenpartners en de werkinstructies voor de uitvoerende ambtenaren.

Het protocol beschrijft overigens niet *alle* elementen uit de Wivvg. Een aantal elementen uit de wet heeft namelijk niet betrekking op de identiteitsvaststelling ten behoeve van de keten als geheel, maar alleen op onderdelen van de keten. Dit betreft bijvoorbeeld het nemen van handpalmafdrukken en de overige "maatregelen in het belang van het onderzoek" ex art. 61a WvSv, en het nemen van vingerafdrukken door DJI ten behoeve van het eigen interne bedrijfsproces. Deze elementen komen *niet* terug in dit protocol.

1.3 Definities
Voor de toepassing van dit Protocol worden de volgende begrippen gehanteerd:

administratieve identiteit: de set van gegevens die omtrent een persoon zijn opgenomen in de basisregistratie Personen (BRP), het Register Niet-Ingezetenen (RNI) als onderdeel van de BRP, de basisvoorziening Vreemdelingen (BVV) of een met deze registers vergelijkbaar buitenlands register, an wel de gegevens omtrent een persoon die zijn opgenomen in een wettig identiteitsbewijs. Deze set van gegevens wordt ook wel aangeduid als: de personalia van een persoon.
biometrie: het gebruik van foto's en/of vingerafdrukken van een persoon ten behoeve van de identiteitsvaststelling.
biometrische identiteit: een unieke set van onveranderlijke dan wel langdurig stabiele fysieke kenmerken van een persoon.
BVID: Basis Voorziening Identificatie. Dit is de software die wordt gebruikt bij de bediening van de ID-zuil identiteit een set van gegevens waaronder een verdachte of veroordeelde uniek geïdentificeerd wordt in de strafrechtsketendatabank (SKDB).
identificeren, identificatie: identiteitsvaststelling ten aanzien van een verdachte of veroordeelde bij het eerste contactmoment in een strafrechtelijk traject.
identificerend persoonsgegeven: elk (relatief) onveranderlijk of voor langere tijd stabiel persoonsgegeven dat dienstig is of kan zijn om de identiteit van een persoon uniek vast te stellen.
Identiteitsvaststelling: het vaststellen wie iemand is met het oog op een in de strafrechtsketen te nemen beslissing of te verrichten handeling. Identiteitsvaststelling kent twee vormen: identificatie en verificatie.
ID-staat: formulier met identificerende persoonsgegevens dat wordt samengesteld vanuit de ID-zuil.
ID-zuil: een technische voorziening die is ontworpen voor de identiteitsvaststelling binnen het strafrecht en het vreemdelingenrecht. De software voor deze zuil wordt BVID genoemd.
Personalia: de gegevens waaronder een persoon wordt aangeduid in een bestand, zoals: naam, adres, woonplaats, geboortedatum, geboorteplaats, status.
registreren, registratie: opnemen van gegevens omtrent een persoon in een bestand (register) (met "registratie" wordt soms gedoeld op de opgenomen set gegevens zelf).
strafrechtsketen: het proces van toepassing van het strafrecht, bestaande uit de stappen opsporen, vervolgen, berechten en tenuitvoerleggen.
strafrechtsketendatabank (SKDB): het centrale bestand van de identificerende administratieve persoonsgegevens en foto's van verdachten en veroordeelden in de strafrechtsketen
strafrechtsketennummer (SKN): het nummer waaronder verdachten en veroordeelden in de SKDB uniek worden aangeduid.
Traject: de gang van een individuele zaak resp. justitiabele door de keten naar aanleiding van een specifiek delict (of verdenking).
verifiëren, verificatie: identiteitsvaststelling ten aanzien van een verdachte of veroordeelde bij een later contactmoment in dezelfde zaak waarin de identificatie heeft plaatsgevonden.
Verificatiemodule: (a) een opstelling van een computer met daaraan gekoppeld een apparaat voor het digitaal nemen van één of twee vingerafdrukken; (b) de software (BVID).

Enkele van de hierboven gegeven definities worden hieronder nader toegelicht:

Persoonsgegeven, identificerend persoonsgegeven:
De term "persoonsgegeven" is ruimer dan "personalia" of "identificerend persoonsgegeven". Een "persoonsgegeven" is elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon (art. 1 sub 1 Wjsg); dus niet alleen de personalia.

De "identificerende" persoonsgegevens kunnen fysiek of administratief van aard zijn. In beide gevallen gaat het om relatief onveranderlijke gegevens. In onderstaand schema worden enkele voorbeelden gegeven:

	(relatief) veranderlijk	(relatief) onveranderlijk = "identificerende persoonsgegevens"
fysiek	kleur van het haar haardracht	geslacht vingerafdrukken gelaatskenmerken tatoeages gebitskenmerken

		iris
		DNA
administratief	adres	naam
	woonplaats	geboorteplaats en -land
	postadres	geboortedatum
		nationaliteit

SKDB, SKN
Voor de strafrechtsketen wordt een centraal bestand van identificerende administratieve persoonsgegevens en foto's van verdachten en veroordeelden opgebouwd: de strafrechtsketendatabank (SKDB; zie artikel 27b, vierde lid, WvSv). Er is een algemene maatregel van bestuur opgesteld waarin de gegevens worden aangewezen die in de SKDB worden opgenomen (Stb. 2009, 352). Ook het strafrechtsketennummer (SKN) heeft een wettelijke grondslag (artikel 27b, eerste lid, WvSv). Het gebruik ervan binnen de strafrechtsketen is verplicht krachtens het derde lid van artikel 27b. De uitgifte van SKN's en het beheer van de SKDB worden behandeld in hoofdstuk 4 van dit protocol.

Identiteit
Een identiteit is een set van gegevens die onder één SKN is gebracht. De optimale identiteitsvaststelling in de strafrechtsketen omvat de administratieve én de biometrische identiteit. De eigen opgave van de betrokkene kan worden getoetst aan zijn administratieve gegevens. Het identiteitsbewijs bevat administratieve gegevens alsmede een foto en bij een aantal identiteitsbewijzen ook een aanduiding van de lengte van betrokkene. Foto's en vingerafdrukken zijn naar verhouding de krachtigste middelen om een verband te leggen tussen een fysieke persoon en de over hem of haar opgeslagen gegevens. Als in een zaak op geen enkele wijze binnen een redelijke termijn de administratieve identiteit van de verdachte te achterhalen is, kan de strafrechtsketen desnoods ook werken met alleen een fysieke

(biometrische) identiteit, bijvoorbeeld in het geval van dagvaarding op signalement.[4]

Identiteitsvaststelling, registreren, identificatie, verificatie
Identiteitsvaststelling kent twee vormen: identificatie en verificatie.

Identificatie is een activiteit van een opsporingsambtenaar (politie, KMar, BOD, BOA). Identificatie houdt in dat ten behoeve van de toepassing van het strafrecht wordt vastgesteld *wie* de betrokkene is. Zij kan worden uitgevoerd met of zonder gebruikmaking van foto en vingerafdrukken. Zij vindt plaats bij het eerste contactmoment naar aanleiding van een vermoedelijk gepleegd strafbaar feit, dus bij ieder nieuw delict (iedere nieuwe verdenking). Dat eerste contactmoment zal meestal zijn de staandehouding of aanhouding van een verdachte in de zin van het Wetboek van Strafvordering. Staandehouding geschiedt op straat en heeft uitsluitend ten doel de identiteit van een verdachte vast te stellen op basis van een aantal administratieve gegevens (art. 52 WvSv). Aanhouding betekent het overbrengen van de verdachte naar een plaats voor verhoor (art. 53-54 WvSv).[5]

Verificatie heeft betrekking op een interventie die later in het traject wordt verricht. Verificatie houdt in dat wordt vastgesteld *of* de persoon die bij een contactmoment in de keten verschijnt, de juiste persoon is, d.w.z. degene die eerder in het traject als verdachte is geïdentificeerd. Het SKN is in die gevallen al tevoren bekend (en de personalia meestal ook). Ook is al tevoren bekend of van betrokkene reeds vingerafdrukken zijn opgenomen in het vingerafdrukkenbestand.

Registratie in de SKDB is mogelijk bij identificatie mét of zónder gebruikmaking van vingerafdrukken. Registratie in de SKDB geschiedt – met inachtneming van de wettelijke bewaartermijnen van de desbetreffende gegevens - in beginsel slechts eenmaal, namelijk bij de eerste keer dat iemand wordt geïdentificeerd. Als een verdachte meer dan eenmaal is geïdentificeerd (zonder resp. met gebruikmaking van biometrie), worden die identiteiten in de SKDB aan elkaar gekoppeld

overeenkomstig de principes die zijn geformuleerd in hoofdstuk 2 van dit protocol en op zodanige wijze dat kenbaar is wat de grondslag is van de identificatie en van de koppeling.

1.4 Systematiek van identiteitsvaststelling
Identificatie kan worden uitgevoerd zonder of met gebruikmaking van foto en vingerafdrukken.

- Identificatie zónder gebruikmaking van foto en vingerafdrukken houdt in het vaststellen van iemands identiteit op basis van (afgezien van de eigen opgave van de betrokkene) alleen een identiteitsdocument in de zin van de Wet op de identificatieplicht (WID). Dit wordt, in de gevallen dat de identificatie wordt uitgevoerd op een bureau, met apparatuur (documentscanner) ondersteund. Er wordt dan een check uitgevoerd op de SKDB en andere registers (BVBSN, NSIS). In de overige gevallen ontstaat het contact met de SKDB pas als ter zake van het vermoedelijk gepleegde strafbare feit proces-verbaal wordt opgemaakt. Blijkt betrokkene nog niet bekend in de SKDB, dan wordt hij geregistreerd zónder dat foto en vingerafdrukken van hem genomen zijn.

- Bij identificatie mét gebruikmaking van foto en vingerafdrukken wordt (geautomatiseerd) nagegaan of de betrokkene al in de SKDB bekend is. Blijkt betrokkene nog niet bekend, dan wordt hij terstond geregistreerd.

- In de Wivvg is de volgende systematiek van ID-vaststelling voorzien.

- Bij het eerste contactmoment in een strafrechtelijk traject, dus in geval van staandehouding of aanhouding of bij enig ander (eerste) verhoor van een verdachte door een opsporingsambtenaar, wordt betrokkene gevraagd naar zijn personalia. De verdachte is niet verplicht tot antwoorden (art. 29, eerste lid, WvSv), óók niet op vragen naar zijn personalia.

- In geval van aanhouding op verdenking van een misdrijf waarvoor *geen* voorlopige hechtenis is toegelaten, geschiedt de identificatie in beginsel aan de hand van een echt, eigen, geldig en gekwalificeerd identiteitsbewijs (= procedure 1).

- In geval van aanhouding of verhoor op verdenking van een misdrijf waarvoor *wel* voorlopige hechtenis is toegelaten, wordt bij het eerste contactmoment door middel van de vingerafdrukken nagegaan of betrokkene al op basis van vingerafdrukken is geregistreerd. Is dat niet het geval, dan wordt hij alsnog geregistreerd. Is betrokkene eenmaal *bekend* in de SKDB, dan kan hij bij elke volgende gelegenheid, hetzij in het lopende traject, hetzij in volgende trajecten (d.w.z.: naar aanleiding van nieuwe strafbare feiten), worden *herkend*.

- Het vorenstaande is ook van toepassing in alle gevallen waarin, zonder dat sprake is van een misdrijf waarvoor voorlopige hechtenis is toegelaten, bij een opsporingsambtenaar twijfel bestaat over de identiteit van de verdachte. In die gevallen is echter een bevel nodig van de officier of hulpofficier van justitie. Bij latere contactmomenten in hetzelfde strafrechtelijke traject wordt volstaan met verificatie. Als van de betrokkene reeds vingerafdrukken genomen zijn, wordt de verificatie uitgevoerd aan de hand van de combinatie "SKN + vingerafdruk(ken)" (procedure 2). Zijn van betrokkene nog geen vingerafdrukken bekend, dan wordt de verificatie uitgevoerd aan de hand van een identiteitsbewijs (procedure 1).

Alleen bij het Openbaar Ministerie en de Rechtspraak is dit anders: daar heeft de OvJ c.q. de rechter de bevoegdheid om bij twijfel aan de identiteit van de als verdachte verschenen persoon (voor de OvJ in het kader van een strafbeschikking en voor de rechter op de terechtzitting, in de raadkamer of bij de rechtercommissaris) de verificatie aan de hand van een identiteitsdocument en/of vingerafdrukken uit te (laten) voeren.

[4] In dat geval wordt de verdachte geregistreerd als "N.N." met vermelding van zijn SKN.

[5] Indien de verdachte wordt uitgenodigd om op het bureau te verschijnen kan dit ook worden aangemerkt als eerste contactmoment.

Met het oog op de verificatie aan de hand van het identiteitsbewijs is de verdachte (of veroordeelde) verplicht een identiteitsbewijs ter inzage aan te bieden indien een rechterlijk ambtenaar of de reclasseringsmedewerker of de medewerkers van de Raad voor de kinderbescherming of de directeur van de penitentiaire inrichting waar hij wordt ingesloten, daar om vraagt.

- Bij eerste insluiting in een penitentiaire inrichting (PI) wordt -ten behoeve van de deugdelijke verbinding met de VVI/SKDB- de identiteit van de in te sluiten persoon geverifieerd op de wijze zoals beschreven (dus P1a of P2). Daarnaast worden bovendien *altijd* foto's en vingerafdrukken genomen voor de eigen interne bedrijfsvoering van DJI conform de Penitentiaire Beginselenwet (art. 28), de Beginselenwet verpleging ter beschikkinggestelden (art 22) en de Beginselenwet justitiële jeugdinrichtingen (art. 33).

De combinatie van middelen leidt tot een aantal onderscheiden procedures, die in hoofdstuk 3 worden beschreven.

1.5 De ketenpartners

De ketenpartners zijn de organisaties die betrokken zijn bij de opsporing, vervolging, berechting en tenuitvoerlegging in het kader van de strafrechtspleging. Zij hebben een gemeenschappelijk belang bij - en dienovereenkomstige verantwoordelijkheid voor - deugdelijke identiteitsvaststelling en registratie van verdachten en veroordeelden overeenkomstig de wet en dit protocol.
De ketenpartners die in de uitvoering van een primaire processen contact hebben met verdachten en veroordeelden (en getuigen) en op wie dus de wet en het protocol van toepassing zijn, zijn:

- de politie
- de Koninklijke Marechaussee
- de vier bijzondere opsporingsdiensten (BOD'en)
- buitengewoon opsporingsambtenaren (BOA's)
- de Rijksrecherche
- het Openbaar Ministerie
- de Rechtspraak
- de Dienst Justitiële Inrichtingen (DJI)
- het NIFP
- de instellingen voor jeugdzorg en/of GGZ *voor zover* zij patiënten of cliënten op strafrechtelijke titel behandelen
- de drie reclasseringsinstellingen (3RO)
- de Raad voor de Kinderbescherming
- instellingen die krachtens de Jeugdwet gecertificeerd zijn om kinderbeschermingsmaatregelen en maatregelen in het kader van de jeugdreclassering te mogen uitvoeren.

[6] Rechter/OvJ: alleen bij twijfel, vgl. art29c Sv.
[7] Rechter/OvJ: alleen bij twijfel, vgl. art29c Sv

Zij moeten handelingen verrichten en beslissingen nemen ten aanzien van verdachten en veroordeelden (en getuigen), en moeten bij gelegenheid van een contactmoment de identiteit van de betrokkene vaststellen.
Daarnaast spelen enkele instanties een ondersteunende rol bij de identiteitsvaststelling, in termen van onderzoek en/of registratie:

- de Landelijke Eenheid van de politie (onderzoeken, registreren en beheren van vingerafdrukken),
- de Justitiële Informatiedienst (beheer SKDB en VVI, toekennen SKN, Matching Autoriteit).

Het NFI onderzoekt, registreert en beheert de DNA-profielen. Medewerkers van het NFI hebben doorgaans alleen contact met justitiabelen in de zin van de wet en dit protocol tijdens het afnemen van het celmateriaal van de veroordeelde. Het NFI werkt conform de Wivvg met het SKN.

Door medewerkers van het CJIB worden verdachten en/of veroordeelden telefonisch gehoord, maar daarbij kan geen sprake zijn van het overleggen van een identiteitsbewijs, het vergelijken van personen met in het dossier van hen aanwezige foto's of het verifiëren van vingerafdrukken. Ook voor zover door medewerkers van het CJIB verdachten en/of veroordeelden aan de balie te woord gestaan worden, is er doorgaans geen sprake van een in de wet voorzien moment van verificatie. Toepassing van het protocol is in die situaties dus niet aan de orde. Wel werkt het CJIB conform de Wivvg met het SKN voor zover het verdachten en veroordeelden betreft.

2 Algemene uitgangspunten

De grondslag van de wet (Wivvg) - en daarmee ook van dit protocol - is:

- dat bij het eerste contactmoment in een strafrechtelijk traject de identiteit van de verdachte eenduidig voor heel de keten wordt vastgesteld en vastgelegd (= identificatie),

- dat die identiteit wordt gekoppeld aan een uniek en door alle organisaties binnen de keten verplicht te gebruiken nummer (= het SKN),

- dat bij een aantal latere contactmomenten in hetzelfde strafrechtelijke traject de identiteit wordt geverifieerd (= verificatie), en

- dat in meer gevallen dan voorheen voor de identificatie en verificatie gebruik wordt gemaakt van identiteitsbewijzen, foto's en vingerafdrukken.

De volgende uitgangspunten en ontwerpbeslissingen liggen voorts ten grondslag aan (de wet en) dit protocol.

a. Er is een centraal bestand met identificerende en andere administratieve persoonsgegevens van verdachten en veroordeelden voor de strafrechtsketen: de strafrechtsketendatabank (SKDB). In het Bivv[8] worden de gegevens aangewezen die in de SKDB moeten en mogen worden opgenomen. Voor de identificatie en verificatie van personen in de strafrechtsketen maken alle ketenpartners gebruik van dit centrale bestand. Het bevat tevens de foto's van verdachten en veroordeelden die overeenkomstig dit protocol zijn genomen ten behoeve van identiteitsvaststelling voor de keten.

b. Er is een centraal bestand met vingerafdrukken van verdachten en veroordeelden ten behoeve van identiteitsvaststelling voor de strafrechtsketen.[9] Dit bestand bevat de (sets van) vingerafdrukken die overeenkomstig het WvSv en dit protocol zijn genomen ten behoeve van de identiteitsvaststelling voor de strafrechtsketen.

c. Iedere verdachte krijgt een SKN. Alle gegevens in de SKDB en in het vingerafdrukkenbestand die betrekking hebben op éénzelfde persoon worden opgenomen onder dit SKN. Het SKN is het verbindingspunt tussen de geregistreerde identiteit en de over die persoon opgenomen gegevens in de diverse bestanden in de keten. Het wordt toegekend door de MA en alleen gebruikt voor:

- communicatie tussen de functionarissen c.q. organisaties binnen de keten, of voor

- gegevensuitwisseling tussen de SKDB en de Basisvoorziening Vreemdelingen (BVV), of voor

- registratie in de eigen bestanden en systemen van ketenpartners.

Voorkomen moet worden dat het nummer gaat circuleren buiten dit door de wet afgebakende domein. Het is daarom ongewenst dat het SKN wordt vermeld op documenten die (alleen) naar burgers (justitiabelen) gaan, zoals brieven, of op documenten die naar instanties buiten de strafrechtsketen gaan. Het nummer bevat geen informatie. Een (nieuw) SKN wordt in beginsel alleen uitgegeven als de betrokkene nog niet eerder conform P3/P4 is geregistreerd. Het SKN wordt ook opgenomen in het vingerafdrukkenbestand en in de DNA-databank van het NFI.

d. Er wordt onderscheid gemaakt tussen het eerste contactmoment en de opvolgende contactmomenten met een verdachte of veroordeelde in een strafrechtelijk traject. De identiteitsvaststelling bij het eerste contactmoment (= identificatie) dient ertoe eenmalig en eenduidig vast te stellen op wie de strafzaak betrekking heeft. De identiteitsvaststelling bij alle opvolgende contactmomenten (= verificatie) dient ertoe te waarborgen dat degene die verschijnt inderdaad degene is die daar en dan moet verschijnen, d.w.z. degene op wie de voorgenomen beslissing of handeling betrekking heeft. Bij alle opvolgende contactmomenten is in de regel tevoren bekend wie op een bepaalde plaats en tijd dient te verschijnen; bij het eerste contactmoment is dat doorgaans niet het geval.

e. De functionarissen die doorgaans als eerste met een verdachte in aanraking komen, zijn de opsporingsambtenaren: politie, Koninklijke Marechaussee, Bijzondere Opsporingsdiensten en BOA's. Zij voeren de identificatie uit en leggen hun verrichtingen en bevindingen vast in het proces-verbaal dat zij opmaken ingevolge art. 152 WvSv.

f. Er wordt onderscheid gemaakt tussen de standaardprocedure voor identiteitsvaststelling en de escalatieprocedure (opschalen bij twijfel, zie par. 3.1 en 4.2). De standaardprocedure bevat vier elementen: de eigen opgave van betrokkene, het identiteitsbewijs, de foto en de vingerafdrukken. De wet bepaalt welk element in welke situatie moet of mag worden ingezet. Een identiteit die conform procedure 3 of 4 van dit Protocol is vastgesteld op basis van een echt, eigen, geldig en gekwalificeerd ("EEGG") ID-bewijs, mét foto en vingerafdrukken, wordt wel aangeduid als een "gevalideerde" identiteit.

g. De opsporingsambtenaar die bij gelegenheid van het eerste contactmoment de identiteit van een verdachte vaststelt (identificatie), gebruikt daarvoor uitsluitend de gegevens die hij "vanuit de betrokkene" verkrijgt, dat wil zeggen: uit de verklaring van de verdachte en/of uit een door de verdachte aangeboden of bij hem aangetroffen identiteitsbewijs en/of vanuit de genomen biometrische kenmerken (foto, vingerafdrukken).

8 Besluit identiteitsvaststelling verdachten en veroordeelden (Stb. 2009, 352).
9 Hiermee wordt zowel gedoeld op de Voorziening voor verificatie en identificatie (VVI) als op

HAVANK; deze worden in dit protocol functioneel als één beschouwd.

Hij biedt de aldus door hem verzamelde gegevens aan via de ID-module aan (het vingerafdrukkenbestand en) de SKDB. Het is uitdrukkelijk *niet* de bedoeling dat hij de desbetreffende gegevens ophaalt uit de SKDB of enige andere databank teneinde de registratie daarop te baseren (met voorbijgaan aan de gegevens die "vanuit de verdachte" worden verkregen). Zou dit wel gebeuren, dan zou dit de waarde zowel van de identiteitsvaststelling als van de gegevens in de SKDB ondermijnen. De betrokken opsporingsinstanties borgen dit uitgangspunt in hun procedures, processen en systemen.

h. Indien van een verdachte reeds vingerafdrukken aanwezig zijn, wordt voor de verificatie in de regel gebruik gemaakt van vingerafdrukken. Dit geldt alleen niet voor verhoren door de rechter (op of buiten de terechtzitting) of de officier van justitie (in het kader van de strafbeschikkingen).

i. Registratie van een verdachte in de SKDB houdt in het toekennen van een SKN aan die persoon en het opnemen van de identificerende persoonsgegevens onder dat SKN. Een verdachte wordt geregistreerd als zijn of haar identiteit overeenkomstig de procedures 1, 3 of 4 van dit protocol is vastgesteld. Er zijn echter enkele uitzonderingen op deze regel. Het kan zijn dat een verdachte wordt vervolgd en veroordeeld zonder dat er ooit enig contactmoment in de zin van de wet en het protocol is geweest, onder meer als zonder staandehouding of aanhouding een (mini-)pv wordt opgemaakt en ingestuurd naar het CJIB of het OM; ook in dat geval zal aan die verdachten een SKN moeten worden toegekend. Een derde uitzondering betreft het geval van bekeuring op kenteken overeenkomstig artikel 181 Wegenverkeerswet 1994. Onder de in dat artikel vermelde voorwaarden is de eigenaar of houder van het motorrijtuig strafrechtelijk aansprakelijk. Diens gegevens worden vanuit het kentekenregister (RDW) in de SKDB opgenomen en daaraan wordt een SKN toegekend (voor zover betrokkene nog niet geregistreerd was onder een SKN).

j. Van de vier standaardelementen voor identiteitsvaststelling vormen de foto's en de vingerafdrukken het sterkste verbindingspunt tussen de persoon en diens administratieve identiteit. Van identiteiten die met gebruikmaking van vingerafdrukken zijn vastgesteld, kan met naar verhouding de hoogste graad van waarschijnlijkheid worden vastgesteld dat zij op dezelfde persoon betrekking hebben. Die identiteiten kunnen “hard” gekoppeld worden, zelfs al is er geen EEGG ID-bewijs aanwezig. “Hard koppelen” wil zeggen dat verschillende identiteiten zonder meer onder één

SKN worden gebracht.
Alle andere koppelingen tussen vastgestelde identiteiten zijn “zacht”. “Zacht” koppelen van identiteiten wil zeggen dat een identiteit die zonder gebruikmaking van vingerafdrukken is vastgesteld, wordt gekoppeld aan een identiteit die al eerder - met of zonder gebruikmaking van vingerafdrukken - is vastgesteld; in dat geval worden beide identiteiten onder hetzelfde SKN gebracht, onder vermelding van de grondslag van de identificatie en de koppeling. Een “zachte” koppeling kan ook aan de orde zijn in de situatie dat identiteiten onder verschillende SKN’s (blijken te) zijn geregistreerd terwijl zij waarschijnlijk op dezelfde persoon betrekking hebben; in dat geval wordt er een verbinding gelegd tussen die SKN’s.
Ook bijvoorbeeld de koppelingen met de identiteiten in de BRP, via het BSN, zijn dus “zachte” koppelingen. Dit geldt óók voor de vingerafdrukken die sinds 21 september 2009 ingevolge de herziene Paspoortwet (Stb. 2009, 252) in de paspoorten worden opgenomen, omdat het verband tussen BSN en biometrie slechts indirect wordt gelegd, namelijk via het document. Bovendien zullen ook in die (toekomstige) situatie de vingerafdrukken in verreweg de meeste gevallen niet gelijktijdig met de uitgifte c.q. het toekennen van het BSN aan een persoon worden genomen en geregistreerd,

maar pas jaren later. Het BSN wordt immers in beginsel bij de geboorte toegekend, maar de meeste mensen krijgen pas later een paspoort of IDkaart. Indien daarentegen een verdachte voor de eerste maal met gebruikmaking van vingerafdrukken, dus overeenkomstig P3 of P4, wordt geïdentificeerd, wordt daarbij *terstond* een nieuw SKN uitgegeven en toegekend. Het SKN dat is toegekend op basis van identificatie mét gebruikmaking van vingerafdrukken (conform P3 of P4) is het hoofd-SKN van betrokkene. Eventuele registraties van betrokkene die reeds eerder zijn aangemaakt op basis van een identificatie zónder gebruikmaking van vingerafdrukken (en waaraan al dan niet reeds een SKN is toegekend) worden daar "zacht" aan gekoppeld. Dit geldt ook voor registraties die naderhand eventueel nog plaatsvinden op basis van een identificatie zonder gebruikmaking van vingerafdrukken (dus conform P1). Het oordeel over het leggen van een "zachte" koppeling is voorbehouden aan de MA (zie hst. 4 van dit protocol).

k. In geval van identificatie maakt ook het raadplegen van (authentieke) registers zoals de BRP (bestaande uit GBA-BRP en RNI-BRP) en/of de Basisvoorziening Vreemdelingen (BVV), onderdeel uit van de standaardprocedure.[10]

[10] Op 6 januari 2014 is de Wet basisregistratie personen (Wet BRP) in werking getreden. Deze wet vervangt de Wet gemeentelijke basisadministratie persoonsgegevens (Wet GBA) uit 1994.

l. De verschillende soorten identificerende gegevens (personalia c.q. administratieve gegevens, foto, vingerafdrukken) worden altijd verzameld en vastgelegd op een zodanige wijze dat een onverbrekelijke samenhang tussen deze gegevens is gewaarborgd. Indien vingerafdrukken zijn genomen, wordt een integere, ondubbelzinnige, goed gedocumenteerde en eenvoudig reproduceerbare relatie tot stand gebracht tussen de vanuit de betrokkene verzamelde personalia en diens vingerafdrukken. Deze relatie wordt zorgvuldig, veilig en duurzaam bewaard, zodat de door betrokkene bij gelegenheid van het nemen van de vingerafdrukken gebezigde c.q. opgegeven personalia altijd ondubbelzinnig kunnen worden gerelateerd aan de vastgelegde vingerafdrukken. Indien de verdachte geen verklaring aflegt en/of indien hij geen ID-bewijs overlegt en/of indien geen ID-bewijs bij hem wordt aangetroffen, wordt dit gegeven mét de reden of oorzaak daarvoor eveneens vastgelegd.

m. Bij het nemen van vingerafdrukken vergewist de uitvoerende ambtenaar zich ervan dat de vingertoppen van betrokkene niet gemanipuleerd of beschadigd zijn. Bij inzage van een ID-bewijs gaat de uitvoerende ambtenaar - binnen de hem ter beschikking staande mogelijkheden - na of het ID-bewijs echt, eigen, geldig en gekwalificeerd ("EEGG") is (zie nader par. 3.2).

n. Bij het nemen van een foto en/of het nemen van vingerafdrukken worden in het geval van *identificatie* altijd datum, tijd en locatie, en de eventueel door betrokkene opgegeven en/of op het ID-bewijs gevonden naam vastgelegd en aangeboden aan het vingerafdrukkenbestand.[11] De genomen vingerafdrukken worden vastgelegd in het vingerafdrukkenbestand.

Bij het nemen van vingerafdrukken ter *verificatie* worden alleen datum, tijd en locatie, en het SKN van betrokkene vastgelegd en aangeboden aan het vingerafdrukkenbestand. In dit geval worden géén vingerafdrukken vastgelegd. De verifiërende instantie biedt het SKN plus de vingerafdrukken van betrokkene aan en krijgt de melding terug: hit / no-hit. In het geval van een hit krijgt zij tevens de personalia en de foto te zien. In het geval van een no-hit is de vervolgactie afhankelijk van de aard van de beschikbare informatie.

o. Ingevolge de Wivvg wordt voorafgaand aan afnemen van celmateriaal van een verdachte of veroordeelde ten behoeve van DNA-onderzoek de identiteit van betrokkene geverifieerd met gebruikmaking van vingerafdrukken. In beginsel is P2 toereikend (het SKN is immers reeds bekend), mits van

De BRP bestaat uit twee delen: een ingezetenen-deel (het oude GBA-deel) en een nietingezetenen-deel t.w. het Register Niet Ingezetenen (RNI).

[11] In het Bivv zijn de gegevens aangewezen die moeten resp. mogen worden opgenomen.

betrokkene reeds vingerafdrukken bekend zijn. Zijn nog geen vingerafdrukken bekend, dan dient P3 en/of P4 (en eventueel P5) te worden

uitgevoerd.
p. De organisatie of functionaris die de identiteit van een verdachte of veroordeelde vaststelt, is verantwoordelijk voor de kwaliteit van de daartoe gebezigde gegevens. De officier van justitie bewaakt en toetst de kwaliteit van de gegevens omtrent de identiteitsvaststelling in de door hem te behandelen strafzaak.
q. De gegevens waarop de identiteitsvaststelling is gebaseerd, worden in de SKDB vermeld op een zodanige wijze dat elke functionaris in de strafrechtsketen daar indien nodig snel en op eenvoudige wijze kennis van kan nemen.
r. Indien met betrekking tot een geregistreerde persoon twijfels bestaan of twijfels rijzen omtrent de juistheid of de betrouwbaarheid van een of meer van de opgenomen identificerende persoonsgegevens en dienaangaande geen voldoende opheldering kan worden bereikt, wordt daarvan in de SKDB aantekening gemaakt op een zodanige wijze dat dit bij het raadplegen van de databank kenbaar is. Dit kan zich bijvoorbeeld voordoen als in het kader van een identiteitsonderzoek een geregistreerde opduikt als mogelijke betrokkene bij of slachtoffer van een identiteitsverwisseling of –fraude.
s. Alle verzamelde identificerende persoonsgegevens - ook eventuele aliassen, valse ID-bewijzen en andere onjuist gebleken gegevens - worden in de SKDB bewaard[12] ten behoeve van eventueel later onderzoek. Indien een identificerend en/of een administratief gegeven omtrent een geregistreerde persoon wordt gewijzigd of gecorrigeerd, wordt het oude gegeven nooit weggegooid of overschreven, maar als "verschijningsvorm" of "alias" of onder een andere vergelijkbare aanduiding bewaard in de centrale bestanden (de SKDB, het vingerafdrukkenbestand).
t. Indien wordt vastgesteld of vermoed dat een verdachte, veroordeelde of getuige valse gegevens heeft opgegeven bij de identiteitsvaststelling, of gebruik heeft gemaakt van een andere dan de eigen identiteit, wordt daarvan altijd proces-verbaal opgemaakt (door een opsporingsambtenaar) of aangifte gedaan (door andere functionarissen). Indien een gesignaleerd of vermoedelijk vals identiteitsbewijs wordt aangetroffen, wordt dit in beslag genomen. Vervalsing van of manipulatie met een identiteitsbewijs wordt gemeld aan de uitgever van het ID-bewijs.
u. Indien de verdachte of veroordeelde vreemdeling blijkt te zijn in de zin van de Vreemdelingenwet 2000, neemt de functionaris die de identiteitsvaststelling uitvoert contact op met de diensten en/of

[12] Ongeacht hoe de informatie - al dan niet geautomatiseerd - tot de SKDB komt.

functionarissen die met de uitvoering van deze wet zijn belast. Het strafrechtelijke traject wordt intussen voortgezet. Het Protocol vreemdeling in de strafrechtsketen (VRIS) wordt gevolgd. Er wordt een onderzoek ingesteld naar de nationaliteit en de verblijfsrechtelijke positie van betrokkene. Het vreemdelingennummer wordt opgenomen in de SKDB en het SKN wordt (conform art. 27b, tweede lid, WvSv) opgenomen in de BVV.
v. Indien een ketenpartner van oordeel is dat een geregistreerde identiteit geheel of gedeeltelijk moet worden gewijzigd, dan wel vermoedt of vaststelt dat een verdachte valse gegevens heeft opgegeven bij de identiteitsvaststelling, dan wel vermoedt of vaststelt dat een verdachte zich in het verleden van valse personalia of valse identiteiten (aliassen etc.) heeft bediend, meldt hij dat aan de MA. Indien een ketenpartner na onderzoek afwijkingen constateert ten opzichte van gegevens die in de BRP zijn opgenomen, meldt hij dit aan de MA. (Afwijkingen ten opzichte van gegevens die in de BVV zijn opgenomen, dienen te worden gemeld aan de politie-eenheid die verantwoordelijk is voor het toezicht op de vreemdeling en aan de MA). De MA beoordeelt de melding en beslist over de noodzaak van nader onderzoek. De MA kan - al dan niet via het OM - de politie of een andere opsporingsinstantie verzoeken om een identiteitsonderzoek uit te voeren. De resultaten van het onderzoek worden aan de MA aangeboden, die beslist over de wijziging van de geregistreerde gegevens. De MA meldt (conform art. 2.34 Wet basisregistratie personen) haar bevindingen aan de gemeente (en/of de BVV of het RNI); tevens koppelt zij aan de instantie die de melding heeft gedaan, het resultaat van haar onderzoek terug. In voorkomende gevallen kan het OM op de voet van art. 1:24 Burgerlijk

Wetboek de Rechtbank verzoeken verbetering van een of meer akten van de burgerlijke stand te gelasten.
w. De ketenorganisaties stellen interne procedures op voor het geval dat de apparatuur die gebruikt wordt voor de identiteitsvaststelling niet of niet naar behoren functioneert, en maken die procedures bekend binnen hun organisatie.

3 Procedures

3.1 Inleiding
In paragraaf 1.2 en 1.3 is aangegeven uit welke vier standaardelementen de identiteitsvaststelling in de strafrechtsketen is opgebouwd en in welke samenhang deze worden ingezet ten behoeve van de identificatie of verificatie. In de gevallen waarin de standaardelementen niet tot opheldering leiden omtrent de identiteit, is nader onderzoek noodzakelijk. De standaardelementen zijn de bouwstenen van de procedures 1 t/m 4, het nader onderzoek wordt in dit protocol aangeduid als procedure 5 (P5).

De samenhang van de procedures is als volgt.
- Procedure 1a is de standaardprocedure voor *identificatie* van een verdachte bij staandehouding en bij aanhouding wegens een feit waarvoor géén voorlopige hechtenis is toegelaten. Slaagt deze procedure niet, dan wordt "opgeschaald" naar procedure 3 (art. 55c, derde lid, WvSv: nemen van vingerafdrukken op bevel van de ovj of hulp-ovj in geval van twijfel over de identiteit).

- Procedure 1b is de standaardprocedure voor *verificatie* van de identiteit van een verdachte of veroordeelde in alle gevallen waarin er nog geen vingerafdrukken van betrokkene zijn opgenomen in de databank.

- Procedure 1c betreft niet een verdachte of veroordeelde, maar een getuige of een opgeëiste persoon die is verschenen voor de rechter en over wiens identiteit twijfel bestaat. Strikt genomen hoort deze procedure niet thuis in dit Protocol. Zij heeft immers niet betrekking op de verificatie van een identiteit in de keten, maar enkel op de vaststelling van de identiteit van een persoon in één schakel van de keten, nl. ten overstaan van de rechter op de zitting of in raadkamer.[13] Om het verschil in uit te voeren handelingen ten aanzien van het ID-bewijs scherp te markeren, wordt deze procedure hier toch kort beschreven.

- Procedure 2 is de standaardprocedure voor *verificatie* van de identiteit van een verdachte of veroordeelde in alle gevallen waarin reeds vingerafdrukken van betrokkene zijn opgenomen in de databank.

- Procedure 3 is in beginsel de standaardprocedure voor het *identificeren* van een verdachte die is aangehouden op of wordt verhoord ter zake van verdenking van een misdrijf waarvoor voorlopige hechtenis is toegestaan.

Daarnaast is deze procedure van toepassing indien de identiteitsvaststelling (identificatie of verificatie) conform P1 of P2 niet is geslaagd.
- Procedure 4 is van toepassing indien de verdachte of veroordeelde nog niet met gebruikmaking van (gerolde) vingerafdrukken is geregistreerd terwijl dat wel voorgeschreven is.

- Procedure 5 is eerst aan de orde indien de overige procedures niet slagen of als er anderszins aanleiding is voor nader onderzoek naar de identiteit.

- Voor een registratie in de SKDB is P1 toereikend indien geen vingerafdrukken voorgeschreven zijn voor de identiteitsvaststelling. Is het gebruik van vingerafdrukken wel voorgeschreven, dan dient registratie te zijn gebaseerd op P3 en P4.

[13] Opsporingambtenaren kunnen op grond van art. 8 Politiewet 2012 een getuige vragen zijn of haar identiteitsbewijs ter inzage aan te bieden.

In de volgende paragrafen worden de genoemde procedures achtereenvolgens beschreven. Waar sprake is van gebruik van apparatuur (voor controle van het document of voor het nemen van foto's of vingerafdrukken) moeten de daarmee verzamelde gegevens (dan wel de apparatuur zelf) voldoen aan de daarvoor door de bevoegde personen of organen vastgestelde (kwaliteits)normen.

3.2 Identificatie en verificatie met ID-bewijs (P1)

Deze procedure kent drie varianten:
1. identificatie van een verdachte (= P1a),
2. verificatie van een verdachte of veroordeelde (= P1b),
3. verificatie door een rechter van de identiteit van een getuige of opgeëiste persoon etc. (= P1c).

De procedure begint in alle gevallen met het vragen naar de naam, voornamen, geboortedatum en geboorteplaats, en eventueel andere personalia, zoals adres van inschrijving in de BRP, woon- of verblijfplaats en eventueel BSN (vgl. art. 27a, 29c, 52, 55c eerste lid WvSv). De verdachte is in geval van verhoor door een opsporingsambtenaar of rechter niet tot antwoorden verplicht (art. 29, eerste lid, WvSv).

In de procedures P1a en P1b wordt de betrokkene gevraagd een identiteitsdocument als bedoeld in artikel 1 van de Wet op de identificatieplicht ter inzage aan te bieden. Indien de verdachte die is staande gehouden of aangehouden (P1a) weigert een ID-bewijs ter inzage aan te bieden, kan hij aan zijn kleding worden onderzocht en kunnen voorwerpen die hij bij zich draagt of met zich mee voert, worden onderzocht (art. 55b WvSv). Leidt dit onderzoek niet tot afdoende opheldering over de identiteit van de verdachte, dan moet de verdachte in beginsel worden aangehouden voor nader identiteitsonderzoek; het oordeel hierover is voorbehouden aan de (hulp-)officier van justitie (art. 55c, derde lid, WvSv). De staande gehouden verdachte die geen ID-bewijs ter inzage aanbiedt, kan ter plekke worden aangehouden wegens (verdenking van) overtreding van artikel 447e WvSr, waarna al hetgeen op de aangehouden verdachte betrekking heeft, van toepassing is.

Inzage van het ID-bewijs houdt in:
a) vergelijken van de foto in het ID-bewijs met de persoon die het ID-bewijs aanbiedt, en
b) vergelijken van de gegevens in het ID-bewijs met die welke (eventueel) door de betrokkene zijn opgegeven.

Tevens wordt het ID-bewijs getoetst op vier vragen (“EEGG”):
1. is het echt,
2. is het eigen,
3. is het geldig,
4. is het gekwalificeerd.

De controle op echtheid behelst een onderzoek naar misbruik, namaak of vervalsing van het ID-bewijs. "Eigen" ziet op de vraag of het ID-bewijs inderdaad betrekking heeft op degene die er gebruik van maakt om zich te identificeren, dan wel is afgegeven aan een andere persoon dan degene die er gebruik van maakt. "Geldig" ziet op de termijn waarvoor het ID-bewijs geldig is. "Gekwalificeerd" wil zeggen: het is een ID-bewijs als bedoeld in artikel 1 van de Wet op de identificatieplicht. Indien een foto en/of vingerafdrukken zijn opgenomen in de chip op het paspoort of reisdocument, mag de opsporingsambtenaar die de identificatie of verificatie uitvoert die biometrische kenmerken gebruiken voor het verifiëren van de authenticiteit van het ID-bewijs ("echt") en de identiteit van de houder ("eigen").[14]
Indien apparatuur voor onderzoek van het ID-bewijs (een documentscanner) beschikbaar is, wordt voorts als volgt gehandeld.

[14] Vgl. art. 4, derde lid, van Verordening (EG) 2252/2004.

a. In het geval van *identificatie* van een verdachte (= P1a) wordt de apparatuur gebruikt om de controle van de echtheid van het ID-bewijs te ondersteunen, om de relevante gegevens uit het ID-bewijs geautomatiseerd over te nemen vanuit de Machine Readable Zone (MRZ) en om een - al dan niet digitale - kopie van het ID-bewijs te maken.

b. In het geval van *verificatie* met betrekking tot een verdachte (= P1b) wordt de apparatuur gebruikt om de controle van de echtheid van het ID-bewijs te ondersteunen en om een - al dan niet digitale - kopie van het ID-bewijs te maken. De geautomatiseerde controle op EEGG wordt echter in beginsel alleen uitgevoerd door opsporingsambtenaren; in alle overige gevallen blijft zij achterwege.

c. Heeft de identiteitsvaststelling niet betrekking op een verdachte of veroordeelde maar op een getuige of opgeëiste persoon (= P1c; deze situatie doet zich alleen voor bij de rechter-commissaris of in de raadkamer of op een terechtzitting of in een uitleveringszaak), dan zal voorshands worden volstaan met inzage c.q. visuele beoordeling van het document; op de rechtbanken en de parketten is er vooralsnog geen apparatuur om de controle van de echtheid van het ID-bewijs te ondersteunen.
De verschillende acties die onder P1 (kunnen) worden uitgevoerd met het ID-bewijs, kunnen met betrekking tot de verschillende categorieën van justitiabelen.

De wijze waarop de controle van het ID-bewijs op de vier criteria EEGG moet worden uitgevoerd, is beschreven in het document "Normen identiteitsvaststelling met behulp van een document".[15] In dat document is ook beschreven welke registers moeten worden geraadpleegd en hoe documentscanners ondersteuning verlenen.
Indien het identiteitsonderzoek naar het oordeel van de onderzoekende ambtenaar positief uitvalt, is daarmee de identiteitsvaststelling voltooid. In het proces-verbaal (of andere document met het oog waarop het identiteitsonderzoek is uitgevoerd)

wordt de uitkomst van het identiteitsonderzoek vastgelegd met vermelding van de aard en het kenmerk van het ID-bewijs waarop dat is gebaseerd.
In geval van twijfel, bijvoorbeeld doordat het onderzoek van het ID-bewijs naar het oordeel van de identificerende opsporingsambtenaar niet positief uitvalt, is nader identiteitsonderzoek noodzakelijk overeenkomstig P3 en/of P4; hiervoor is een beslissing van de officier of hulpofficier van justitie noodzakelijk (art. 55c, derde lid, WvSv).
De procedure voor identiteitsvaststelling met alleen een ID-bewijs, zoals in deze paragraaf beschreven (P1), kan als volgt vereenvoudigd worden samengevat:

3. Verificatie met SKN + vingerafdrukken (P2)

Dit proces houdt in het nemen van één of meer gescande vingerafdrukken ("livescan"). Deze worden mét het SKN digitaal aangeboden aan het vingerafdrukkenbestand, met vermelding van datum en tijd. Het systeem vergelijkt 1:1 en antwoordt binnen enkele seconden of de aangeboden combinatie van

Verzamelen
- vragen naam (etc.) + ID-bewijs;
- evt. onderzoek kleding (etc.)

uitkomst negatief
(of geen ID-bewijs)

Beoordelen
- visuele vergelijking foto
- onderzoek ID-bewijs

15 Normen documentcontrole 1.1. 12 juli 2007 (identiteitsdocumentscanner).

beslissing (hulp-)ovj
(alleen bij P1.a)
Conclusie
ID-onderzoek voltooid,
identiteit is vastgesteld
uitkomst positief
indien op bureau:
gebruik apparatuur ➔
check registers etc.
(in backoffice)

vingerafdruk en SKN reeds als zodanig bekend is ("hit / no hit"). Als dat het geval is, wordt dit teruggemeld en worden de bij de identiteit behorende personalia en foto getoond. Is de aangeboden combinatie niet reeds als zodanig bekend, of wel bekend maar nog niet overeenkomstig de wet en dit protocol vastgesteld, dan is nader identiteitsonderzoek noodzakelijk.
P2 kan als volgt schematisch worden samengevat:

3.4 Identificatie met foto + vingerafdrukken (P3, P4)

Er wordt altijd gestart met het nemen van tien platte vingerafdrukken. Dit gebeurt digitaal ("livescan"). Tevens wordt de verdachte gevraagd naar zijn naam (etc.) en wordt het ID-bewijs ter inzage gevraagd overeenkomstig P1a, en wordt een frontale foto gemaakt.[16] Dit geheel wordt aangeduid als P3.

Verzamelen
- SKN
- vingerafdruk(ken)

Verwerken (in backoffice)
- 1:1 vergelijking
- SKN + v.a. bekend?

melden aan OvJ en/of
MA
Conclusie
verificatie geslaagd ("herkenning") "hit" "no hit" melding vanuit het vingerafdrukkenbestand

Deze procedure heeft als doel om eenvoudig en snel met gebruikmaking van vingerafdrukken de identiteit vast te stellen.
Indien betrokkene op basis van de platte vingerafdrukken niet wordt herkend in het vingerafdrukkenbestand, of indien er ondanks herkenning van de vingerafdrukken twijfel blijft ten aanzien van de juiste identiteit, moeten aanvullend tien gerolde vingerafdrukken worden genomen; een beslissing van een officier of hulpofficier van justitie is hiervoor niet vereist. Dit wordt aangeduid als PP4.[17]
Schematisch ziet de procedure er als volgt uit:
Indien betrokkene op basis van zijn vingerafdrukken wordt herkend, wordt in stap 2 het corresponderende SKN teruggemeld. Indien betrokkene niet wordt herkend,

1. Verzamelen (P3)
- verklaring van verdachte
- inzage + scan ID-bewijs
- 10 platte vingerafdrukken (livescan)

2. Controleren en vastleggen
Gebeurt in backoffice. Antwoord komt binnen enkele minuten.

16 Onder art. 55c WvSv kunnen ook andere dan frontale gelaatsfoto's worden genomen.
17 Procedure 4 wordt alleen uitgevoerd op die locaties waar de benodigde voorzieningen en kennis aanwezig zijn. In het geval van met inkt en papier gerolde vingerafdrukken zal dit voorshands met name op cellencomplexen zijn. Zie de circulaire van de ministers van Justitie

en van Binnenlandse Zaken en Koninkrijksrelaties van 26 mei 2010 over de inwerkingtreding van de Wivvg

3. Beoordelen
Het teruggemelde resultaat beoordelen.
Zo nodig nieuwe foto nemen.

4. Maken vingerslip (P4)
Indien nodig: vingerslip maken en (digitaal) opsturen naar vingerafdrukkenbestand.
Antwoord komt binnen zes uur.

5. Afronden
- printen ID-staat
- indien nodig: starten nader Identiteitsonderzoek

wordt een nieuwe registratie in het vingerafdrukkenbestand en SKDB aangemaakt en een nieuw SKN toegekend en teruggemeld. Indien in P4 blijkt dat de persoon toch al bekend was, wordt dat teruggemeld en zullen de MA en de Landelijke Eenheid van de Politie in onderling overleg de bestaande en de nieuwe registratie aan elkaar koppelen.

Indien de verdachte medewerking weigert of zich eventueel zelfs verzet, kan tegen hem proces-verbaal worden opgemaakt ter zake van overtreding van artikel 184 of 180 WvSr. Maar het verdient uiteraard de voorkeur om te trachten alsnog de foto en vingerafdrukken te nemen, waarbij - binnen de daarvoor geldende regels en voorwaarden - zo nodig dwang kan worden toegepast.
Het resultaat van de identificatie wordt vastgelegd in het systeem en op de ID-staat. De ID-staat vermeldt onder meer:

- datum en tijd van de identiteitsvaststelling,
- zo mogelijk de personalia (eventueel NN) en BSN (en/of eventueel vreemdelingennummer) van betrokkene,
- het SKN,
- de foto,
- enkele gegevens over de opsporingsambtenaar die de identificatie heeft uitgevoerd, en
- de aard van de gegevens (opgave verdachte, ID-bewijs, foto, vingerafdrukken) waarop de uitgevoerde identificatie is gebaseerd.

De ID-staat is een formulier met identificerende persoonsgegevens dat wordt samengesteld vanuit de BVID ('vanaf de zuil') en dat door de opsporingsambtenaar bij het pv/dossier moet worden gevoegd. Het Openbaar Ministerie dient bij de ontvangst van de dossiers te controleren of en zo ja of de juiste ID-staten zijn bijgevoegd. Indien het dossier geen of niet de juiste ID-staat bevat, dient door het OM terstond actie te worden ondernomen om dit (doen) te herstellen.[18]

3.4.1 Identificatie met (foto +) 10 "platte" vingerafdrukken (P3)
Met deze procedure wordt gestart bij een aanhouding of verhoor op verdenking van een VH-misdrijf (en als er bij een niet-VH-delict sprake is van twijfel over de identiteit, naar het oordeel van de officier of hulpofficier van justitie). Zij houdt in:

- vragen naar naam etc. ("eigen verklaring"),
- inzage + controle ID-bewijs,
- nemen van tien digitaal gescande vingerafdrukken ("livescan").

De vingerafdrukken worden digitaal aangeboden aan het vingerafdrukkenbestand, met vermelding van datum en tijd. Het vingerafdrukkenbestand gaat na of de aangeboden set vingerafdrukken reeds bekend is (dit is een 1:n zoeking) en antwoordt binnen ten hoogste enkele minuten. De identificerende opsporingsambtenaar vergelijkt alle verzamelde gegevens (d.w.z.: SKDB + IDbewijs + evt. eigen verklaring).

18 Zie ook 'Richtlijnen voor het vaststellen (en vastleggen) van de identiteit van de verdachte'

in de brief van de Voorzitter van het College van PG's, d.d. 24 juni 2015, kenmerk PaG/B&S/17144, Maatregelen n.a.v. rapport 'Beschikt en Gewogen' van PG HR.

Er zijn twee situaties mogelijk:

1. *Situatie:* Verdachte heeft al een "biometrisch SKN". Het reeds bekende SKN + bijbehorende gegevens (personalia, foto) worden getoond vanuit de SKDB. Verdachte heeft of toont een EEGG identiteitsbewijs en heeft eventueel ook een verklaring afgelegd. Alle verzamelde gegevens stemmen onderling overeen, de getoonde foto is nog goed gelijkend en er is ook overigens geen aanleiding tot twijfel over de identiteit.
Vervolgactie: Geen, identificatie is voltooid.[19]

2. *Situatie:* Er is nog geen volledige registratie, of de getoonde foto is niet of niet meer goed gelijkend, of de reeds geregistreerde gegevens stemmen niet overeen met de vanuit de verdachte verzamelde gegevens.
Vervolgactie: Alsnog volledige registratie dan wel nader identiteitsonderzoek uitvoeren.
Als vermoed wordt dat de verdachte een vreemdeling is, wordt de set vingerafdrukken zowel in het strafrechtelijke vingerafdrukkenbestand als in het vreemdelingenrechtelijke vingerafdrukkenbestand (de BVV) gezocht. Indien reeds vingerafdrukken, genomen krachtens het vreemdelingenrecht, aanwezig zijn in de BVV, worden toch alsnog vingerafdrukken overeenkomstig dit protocol resp. overeenkomstig het WvSv genomen en in het strafrechtelijke vingerafdrukkenbestand opgeslagen. Daarmee wordt voorkómen dat problemen zouden kunnen rijzen doordat vingerafdrukken die in het kader van het vreemdelingenrecht zijn genomen, wellicht niet gebruikt zouden mogen worden in het strafrecht.

3.4.2 Identificatie met foto + 10 "gerolde" vingerafdrukken (P4)

Deze procedure wordt alleen uitgevoerd als in P3 de verdachte niet op basis van zijn vingerafdrukken wordt herkend in het vingerafdrukkenbestand.[20] De vingerafdrukken worden (met inkt op een vingerslip, dan wel digitaal) gerold genomen.
De vingerafdrukken worden, met de eventueel daarbij opgegeven naam (etc.), aangeboden aan het vingerafdrukkenbestand. In het vingerafdrukkenbestand wordt gezocht of de set vingerafdrukken niet toch reeds bekend is. Het resultaat van het onderzoek wordt binnen zes uur teruggemeld aan de opsporingsinstantie die de vingerafdrukken heeft aangeleverd en aan de MA.[21]

3.5 Nader identiteitsonderzoek (P5)

Deze procedure wordt ingezet indien na uitvoering van de hiervóór beschreven procedures twijfel blijft bestaan omtrent de identiteit van de verdachte. Dit kan onder meer het geval zijn indien al wel vingerafdrukken bekend zijn maar nog niet gekoppeld aan een "EEGG" ID-bewijs, terwijl op het moment van identificatie ook niet zo'n document voorhanden is.

[19] N.B.: De komende jaren kan het nog voorkomen dat van een verdachte al wel gerolde vingerafdrukken aanwezig zijn, maar dat hij nog geen biometrisch SKN heeft. In dat geval wordt door de SKDB een nieuw SKN aangemaakt en aan de identificerende ambtenaar teruggemeld. Ook dan geldt dat als alle verzamelde gegevens onderling overeenstemmen en er geen aanleiding is tot twijfel over de identiteit, geen vervolgactie nodig is: de identificatie is voltooid.
[20] Hiermee wordt zowel gedoeld op de Voorziening voor verificatie en identificatie (VVI) als op HAVANK; deze worden in dit protocol functioneel als één beschouwd.
[21] In een aantal gevallen worden de gerolde vingerafdrukken (vingerslips) thans nog per

koerier toegezonden aan de Landelijke Eenheid van de Politie; in dat geval kan het resultaat van het onderzoek uiteraard niet binnen zes uur teruggemeld worden.
Een opsporingsonderzoek is niet afgerond zolang niet voldoende zekerheid is verkregen omtrent de identiteit van de verdachte. Er kan dan gebruik worden gemaakt van de in artikel 61a WvSv vermelde bevoegdheden "in het belang van het onderzoek", alsmede van alle overige wettige opsporingsbevoegdheden.
De onderzoeksresultaten worden vastgelegd in een proces-verbaal van verrichtingen en bevindingen en aangeboden aan de MA, die besluit omtrent opneming in de SKDB. Indien het niet mogelijk is tot afdoende opheldering te komen omtrent de verschillende identiteiten, wordt in ieder geval in de desbetreffende registers bij de desbetreffende identiteiten daarvan melding gemaakt op een zodanige wijze dat dit bij het raadplegen van het bestand kenbaar is.
De partij die het identiteitsonderzoek volgens deze paragraaf uitvoert, legt in het eigen primaire-processysteem vast op basis van welke bronnen de identiteit is vastgesteld. De aard van de documenten en de eventuele combinatie van de gebezigde bronnen worden vastgelegd. Op ketenniveau, d.w.z. in de SKDB, wordt vastgelegd:

- welke organisatie en welke functionaris de identiteit heeft vastgesteld,
- aan welk type documenten de gebruikte gegevens zijn ontleend c.q. op welke gegevens de identiteitsvaststelling is gebaseerd, en
- welke mate van zekerheid resp. waarschijnlijkheid aan de vaststelling kan worden toegekend.

De vastlegging geschiedt op een zodanige wijze dat deze gegevens bij het raadplegen van het bestand kenbaar zijn.

Er kunnen twee aanleidingen zijn om een identiteitsonderzoek zoals in deze paragraaf bedoeld in te stellen. De ene mogelijkheid is dat de politie op eigen initiatief zo'n onderzoek instelt, als bij de identificatie blijkt dat de "standaard"-middelen niet voldoende opheldering bieden over de identiteit van de aangehouden verdachte. De andere mogelijkheid is dat er op enig moment twijfel rijst omtrent een vastgestelde identiteit en dat de MA - al dan niet via het OM - een verzoek doet tot het (doen) instellen van een nader onderzoek naar de identiteit van een geregistreerde verdachte of veroordeelde. In het eerste geval worden de resultaten gemeld aan de MA en verwerkt in het proces-verbaal van de strafzaak dat aan het OM wordt aangeboden. In het tweede geval worden de resultaten aangeboden aan de MA (en onder omstandigheden ook aan het OM dat de opdracht tot onderzoek verstrekte).

3.6 Opleiding, kennis en expertise

Voor de juiste uitvoering van het identificatieproces conform dit protocol is het hebben van het adequate kennis en expertiseniveau van wezenlijk belang. Zowel bij de eerstelijns- als bij de tweedelijns uitvoering dienen de daartoe aangewezen en geautoriseerde professionals op permanente basis geschoold en bijgeschoold te worden via de daartoe geëigende opleidingen en cursussen. Via een gedegen inbedding in de basis-opleiding en door middel van specifieke expert-opleidingen moet structurele aandacht geborgd zijn.

4 Matching

4.1 De Matching Autoriteit: functies en taken

De minister van Justitie en Veiligheid kent aan elke verdachte een SKN toe en beheert de SKDB. De wettelijke taken van de minister met betrekking tot het uitgeven en beheren van het SKN en het beheer van de SKDB worden in mandaat uitgevoerd door de Justitiële Informatiedienst, afdeling Matching (de Matching Autoriteit). Het matchen houdt in dat door de ketenpartijen aangeleverde identificerende persoonsgegevens worden vergeleken met de reeds in de SKDB aanwezige registraties. De MA kan daaraan de conclusie verbinden dat de persoon reeds een SKN heeft, of dat de persoon nog geen SKN heeft; in het laatste geval zal aan betrokkene een SKN worden toegekend. Een verdachte heeft nog geen SKN indien hij nog niet bekend is in de SKDB en/of indien hij nog niet overeenkomstig de wet en het protocol is geïdentificeerd. De matching van vingerafdrukken wordt uitgevoerd binnen het vingerafdrukkenbestand.

In het geval van identificatie zonder gebruikmaking van biometrie (P1) wordt, nadat door een functionaris overeenkomstig de wet en dit protocol de identiteit van een verdachte is vastgesteld, de set van verzamelde gegevens aangeboden aan de SKDB. Daarin wordt nagegaan of betrokkene reeds een SKN heeft. Zo ja, dan meldt de MA het SKN terug aan de functionaris of organisatie die de gegevens had aangeleverd; de aangeleverde set gegevens wordt toegevoegd aan het reeds geregistreerde SKN. Zo nee, dan wordt een nieuw SKN aangemaakt en teruggemeld aan de functionaris of organisatie die de gegevens had aangeleverd.

Indien de identificatie is uitgevoerd met gebruikmaking van vingerafdrukken (P3 en/of P4), wordt in het vingerafdrukkenbestand nagegaan of betrokkene daar reeds geregistreerd is en al een SKN heeft. Indien dat het geval is, wordt het SKN teruggemeld; de aangeleverde set gegevens wordt toegevoegd aan het reeds registreerde SKN (administratieve identificerende persoonsgegevens en foto in de SKDB; de vingerafdrukken in het vingerafdrukkenbestand). Indien de betrokkene nog geen SKN heeft binnen het vingerafdrukkenbestand, worden de verzamelde gegevens aangeboden aan de SKDB en wordt in de SKDB een nieuw SKN aangemaakt en teruggemeld.

Indien de aangeboden administratieve gegevens afwijken van de in de SKDB opgenomen gegevens maar de MA nochtans van oordeel is dat het een reeds onder een SKN geregistreerde persoon betreft, meldt zij het SKN en de reeds geregistreerde gegevens terug aan de aanleverende functionaris of organisatie. Iedere instantie die gegevens verwerkt, is ingevolge de wetgeving (Art. 3 lid 1 Wjsg; artikel 4, eerste lid, Wet politiegegevens) verplicht de nodige maatregelen te treffen opdat de persoonsgegevens die zij verwerkt, juist en nauwkeurig zijn. De aanleverende organisatie neemt derhalve de gegevens uit de SKDB over, óf de aangeleverde gegevens worden in de SKDB toegevoegd aan het reeds bestaande SKN.

Indien naar het oordeel van de MA nader identiteitsonderzoek nodig is, richt zij een daartoe strekkend verzoek tot de desbetreffende opsporingsinstantie. In voorkomende gevallen kan zij ook een verzoek doen aan het OM. De opsporingsinstantie meldt de resultaten van het uitgevoerde onderzoek terug aan de MA.

De MA heeft, uitgaande van de hiervoor geschetste rol en functie[22], de volgende taken:

a. *Uitgifte en beheer van SKN's*: Op basis van de aangeleverde identificerende persoonsgegevens kent de MA een SKN toe aan een identiteit dan wel voegt zij informatie toe aan een reeds bestaand SKN. Indien aan vermoedelijk dezelfde persoon meer dan één SKN is toegekend op basis van verschillende identificaties, beoordeelt de MA de gegevens en legt eventueel koppelingen tussen de verschillende SKN's resp. identiteiten. Identificaties op basis van vingerafdrukken kunnen altijd "hard", dat wil zeggen met maximale mate

van waarschijnlijkheid, aan elkaar gekoppeld worden; deze worden derhalve onder één en hetzelfde SKN gebracht. Identificaties die worden uitgevoerd zónder gebruikmaking van vingerafdrukken zijn "zachter", d.w.z. zij hebben een mindere mate van waarschijnlijkheid, en kunnen leiden tot meer dan een SKN; de verschillende SKN's worden dan ook "zacht" gekoppeld. Indien een identificatie is uitgevoerd mét gebruikmaking van vingerafdrukken is deze leidend en worden de SKN's die reeds zijn toegekend op basis van identificatie zónder vingerafdrukken (en de bij die SKN's behorende gegevenssets) daar "zacht" aan gekoppeld.

b. *Beoordelen*: De MA beoordeelt de ter identificatie of verificatie aangeleverde gegevens marginaal. Onder meer toetst zij of de gegevens compleet zijn en of de juiste bronnen gehanteerd zijn (eigen opgave van betrokkene, IDbewijs, foto, vingerafdrukken). Zij gaat daarbij uit van de door de identificerende instantie gekozen procedure. Het is niet aan de MA om te beoordelen of de identificerende instantie de juiste procedure heeft gekozen; dat oordeel komt toe aan het OM. Voorts checkt zij de gegevens op de BRP () of op de BVV (indien een V-nummer bekend is) en/of andere registers. Zo nodig informeert zij de aanleverende instantie over haar bevindingen.

c. *Registreren*: De MA registreert de identificerende persoonsgegevens (inclusief foto maar exclusief de vingerafdrukken) in de SKDB en kent een SKN toe aan naar haar oordeel nieuwe identiteiten. Voorts pleegt zij onderhoud op de verwerkte gegevens door wijzigingen vanuit de BRP of BVV door te voeren of door het resultaat van een uitgevoerd identiteitsonderzoek door te voeren. Eventuele wijzigingen in geregistreerde gegevens meldt zij aan de ketenpartners die daar belang bij hebben.

d. *Behandelen verzoeken tot inzage, correctie etc*.: Personen die menen onjuist of ten onrechte geregistreerd te staan in de SKDB (al dan niet als gevolg van identiteitsfraude), kunnen zich wenden tot de minister van Justitie en Veiligheid met een verzoek om inzage dan wel correctie van geregistreerde gegevens (art. 18 Wjsg). De MA behandelt namens de minister deze verzoeken. Betreft het verzoek of de klacht een bestand dat niet door de MA wordt beheerd, dan geleidt zij de klacht door naar de verantwoordelijke voor het desbetreffende bestand. De MA draagt naar vermogen bij aan een praktische en effectieve oplossing van het gerezen probleem. Voor zover mogelijk worden verzoeken informeel afgehandeld. Wijzigingen in vastgelegde gegevens worden gelogd.

e. *Beheer SKDB*: De MA is belast met het operationele beheer van de SKDB. Zij bewaakt binnen de grenzen van haar mogelijkheden en bevoegdheden de juistheid van de in de SKDB opgenomen gegevens (vgl. art. 3 eerste lid Wjsg). Zij oordeelt over het al dan niet leggen van koppelingen tussen identiteiten in de SKDB. Bij meldingen van (ontdekt) gebruik van valse identiteiten, aliassen e.d. documenteert zij deze en beoordeelt ze op hun consequenties voor reeds bestaande registraties. Dit leidt tot het "schonen" van de SKDB (en van de daaraan via de SKN's gekoppelde justitiële documentatie). De raadplegingen van de SKDB worden vastgelegd ("gelogd"). De Justitiële Informatiedienst informeert de ketenorganisaties als zij afwijkende patronen in het raadplegen van de SKDB waarneemt.

f. *Ondersteunen*: De MA ondersteunt de ketenpartners bij het vaststellen van identiteiten (zowel identificeren als verifiëren) door middel van een helpdesk. Indien de ketenpartner vragen heeft over een gegeven in de SKDB, kan hij de helpdesk raadplegen. Indien een ketenpartner twijfels heeft omtrent de identiteit van een verdachte of veroordeelde, dient hij de MA te verwittigen. De ketenpartijen geven aan wie zij daartoe autoriseren. Elke organisatie wijst een contactpersoon aan die kan fungeren als aanspreekpunt voor de MA.

22 De in dit hoofdstuk geschetste rol en functie van de MA doet geen afbreuk aan de wettelijke bevoegdheden van de rechter krachtens het Wetboek van Strafvordering, zie onder meer de artikelen 579-584 van dat wetboek (het rechtsgeding tot herkenning van veroordeelden of van

andere gevonniste personen).

g. *Coördineren*: De MA coördineert nadere onderzoeken naar de identiteit van verdachten en veroordeelden. Indien vanwege twijfel over een identiteit een nader onderzoek wordt uitgevoerd, bewaakt de MA de voortgang daarvan.

h. *Signaleren*: De MA informeert zowel binnen de keten als daarbuiten belanghebbende instanties over (vermeende) fouten in persoonsregistraties. Indien zij constateert dat de registratie van een justitiabele in de BRP onjuist is, meldt zij dit – via de zgn. Terugmeldvoorziening - aan de desbetreffende gemeente. Bij geconstateerde fouten in de BVV wordt DRM (Directie Regie Migratieketen) of de IND geïnformeerd. Indien er twijfel bestaat over de juistheid van gegevens in de SKDB zelf, kan de MA het OM verzoeken een identiteitsonderzoek te laten uitvoeren. Het OM beslist of het de politie/KMar opdracht geeft voor een nader identiteitsonderzoek. De MA informeert de officier van justitie als zij waarneemt dat een DNA-profiel is vastgesteld zonder dat de identiteit van betrokkene is geverifieerd via diens vingerafdrukken resp. dat een DNA-nummer is toegekend zonder dat er een vingerafdrukken-nummer is.

i. *Rapporteren*: De MA volgt de ontwikkelingen met betrekking tot uitvoering van de wet en het Protocol. Zij rapporteert jaarlijks aan de minister van Justitie en Veiligheid over haar verrichtingen en legt daarover verantwoording af. Tevens rapporteert zij aan de minister over haar bevindingen ten aanzien van de identiteitsvaststelling van verdachten en veroordeelden in de strafrechtsketen. Onderdeel van deze rapportage is het geven van een beeld van de ontwikkelingen met betrekking tot het gebruik van valse identiteitsbewijzen, personalia en identiteiten (aliassen en dergelijke) in de strafrechtsketen.

4.2 Matching en de opvolging daarvan

Elke verdachte krijgt ingevolge de Wivvg één – en niet meer dan één - SKN.[23] Het SKN is de kapstok voor de identificerende persoonsgegevens in de SKDB (en het vingerafdrukkenbestand) en de sleutel tot de gegevens in de bestanden van de strafrechtsketen. Aan een SKN kunnen echter uiteenlopende sets van identificerende persoonsgegevens hangen. Immers, de identiteit van een verdachte of veroordeelde wordt op verschillende momenten vastgesteld, hetzij binnen één traject (naar aanleiding van één en hetzelfde strafbaar feit) of binnen meer dan één traject (naar aanleiding van verschillende strafbare feiten). Ook kan het voorkomen dat niet voldoende uitsluitsel kan worden verkregen over de juistheid van gegevens of dat op eenzelfde contactmoment diverse onderling niet consistente gegevenselementen

betreffende de identiteit van de betrokkene worden verzameld. Bijvoorbeeld: er wordt een verschil geconstateerd tussen de eigen opgave van de verdachte en/of een door hem overgelegd of bij hem aangetroffen identiteitsdocument en/of de personalia die over hem eerder zijn vastgelegd in het vingerafdrukkenbestand. En ten slotte kunnen verschillende functionarissen of organisaties onder omstandigheden verschillend oordelen over de juistheid, betrouwbaarheid en/of actualiteit van een of meer gegevens.

In beginsel wordt voor de identiteitsvaststelling het minst bezwarende middel ingezet: de standaardprocedure. Leidt de standaardprocedure echter niet tot afdoende opheldering omtrent de identiteit van betrokkene, dan wordt opgeschaald (geëscaleerd) naar een zwaardere procedure. Het oordeel hierover ligt in eerste instantie bij de uitvoerende ambtenaar. In geval van twijfel raadpleegt deze zijn

[23] Het kan ingevolge dit Protocol voorkomen dat aan een verdachte of veroordeelde meer dan één SKN is toegekend. In dat geval wordt één SKN als het "hoofd-SKN" aangemerkt. Alle zoekacties in de SKDB komen in eerste instantie uit bij dit hoofd-SKN. Alle overige eventueel toegekende SKN's worden aan het hoofd-SKN gehangen, zie hst. 2, uitgangspunt j.

leidinggevende. In het geval van *identificatie* bij een verdachte ter zake van een niet-VH-delict is het oordeel in geval van twijfel voorbehouden aan de officier of hulpofficier van Justitie (art. 55c, derde lid, WvSv). "Opschalen" houdt voor de politie (en KMar) in dat zij zelf een nader identiteitsonderzoek instelt; zij stelt de Matching Autoriteit hiervan op de hoogte. Voor de rechter op de terechtzitting houdt het in dat hij een nader onderzoek naar de identiteit van de als verdachte verschenen persoon kan uitvoeren of gelasten (art. 273, eerste lid, tweede volzin, WvSv; hetzelfde geldt voor de officier van justitie in het kader van de OM-afdoening op grond van artikel 29c); dit onderzoek zal doorgaans worden uitgevoerd door de parketpolitie (of een daarmee vergelijkbare organisatie). Voor alle overige ketenpartners houdt "opschalen" in het informeren van de Matching Autoriteit. Leidt de twijfel omtrent de identiteit er echter toe dat de strafzaak "uit de rails loopt", bijvoorbeeld doordat een taakstraf niet kan worden tenuitvoergelegd, dan dient ook de minister van Justitie en Veiligheid en waar nodig het Openbaar Ministerie (i.c. de officier van justitie) te worden verwittigd.[24]

In alle gevallen worden de sets van identificerende gegevens opgenomen in de SKDB. In de SKDB wordt tevens vastgelegd:

- op welke gegevens de ID-vaststelling is gebaseerd; *alle* vanuit de betrokkene verzamelde gegevens of gegevenselementen worden vastgelegd, ook al zijn deze eventueel onderling niet consistent;

- waar, wanneer en door wie de ID-vaststelling is uitgevoerd.

Nieuw aangeboden sets worden vergeleken met reeds geregistreerde sets (= matching). In de meeste gevallen zal een van de sets gegevens door de Matching Autoriteit worden aangemerkt als leidend. Dit oordeel berust op de resultaten van het door de opsporingsambtenaar uitgevoerde identiteitsonderzoek, waar nodig aangevuld met eigen administratief onderzoek door de Justitiële Informatiedienst. Allereerst moet worden vastgesteld of de verschillende sets van gegevens betrekking hebben op dezelfde persoon. Dit wordt door de Justitiële Informatiedienst bepaald aan de hand van (achtereenvolgens) de volgende criteria:

- vingerafdrukken. Of de verschillende sets van gegevens betrekking hebben op dezelfde persoon wordt in dit geval - geautomatiseerd of handmatig - vastgesteld door (de operationele beheerder van) het vingerafdrukkenbestand.
- (forensische) foto (dus niet pasfoto o.i.d.);
- BSN of Vreemdelingennummer;
- naam, geboortedatum en -plaats, adres, etc. (volgens vastgestelde algoritmen);
- documentnummer;
- overige eventueel beschikbare gegevens.

Nadat is vastgesteld dat verschillende sets personalia betrekking hebben op dezelfde persoon, stelt de MA vast welke set van personalia leidend is. Hij doet dit aan de hand van (achtereenvolgens) de volgende criteria:

- Indien de identiteit is vastgesteld op basis van P3 (vingerafdrukken + EEGG ID-bewijs) wordt het resultaat daarvan als leidend aangemerkt (= "gevalideerde identiteit").

[24] Door de inwerkingtreding Wet herziening tenuitvoerlegging strafrechtelijke beslissingen (Wet USB) per 1-1 2020 verschuift de formele verantwoordelijkheid over de executie van rechterlijke beslissingen van het OM naar de minister van Justitie en Veiligheid. Hierdoor komt de regie op de tenuitvoerlegging bij de Minister van Justitie en Veiligheid te liggen. De coördinatie van de feitelijke tenuitvoerlegging van strafrechtelijke beslissingen wordt centraal belegd bij een uitvoeringsdienst van het Ministerie van Veiligheid en Justitie, te weten het Centraal Justitieel Incassobureau (verder: CJIB). Met de inwerkingtreding van de wet USB verstrekt het openbaar ministerie alle voor tenuitvoerlegging vatbare beslissingen aan de Minister. Daarnaast blijft het openbaar ministerie verantwoordelijk voor specifieke taken binnen de tenuitvoerlegging, zoals het waar nodig in het kader van de tenuitvoerlegging

aanbrengen van zaken bij de strafrechter, teneinde deze een vervolgbeslissing te laten nemen.

- Indien het resultaat van nader identiteitsonderzoek volgens P5 (zonder EEGG ID-bewijs) beschikbaar is, wordt dit als leidend aangemerkt.
In beide gevallen geldt dat indien de Matching Autoriteit meent te moeten afwijken van de bevindingen van de opsporingsinstanties, zij contact opneemt met de desbetreffende opsporingsinstantie en hierover in gesprek gaat.
- Indien geen vingerafdrukken en ook geen resultaten van nader identiteitsonderzoek volgens P5 beschikbaar zijn, bepaalt de Justitiële Informatiedienst op basis van de door hem gehanteerde algoritmen en criteria welke set van gegevens als leidend moet worden aangemerkt. Deze algoritmen en criteria worden beoordeeld in de periodieke audits die worden uitgevoerd ter zake van de naleving van dit Protocol (zie par. 1.1).

De ketenpartijen die zijn aangesloten op de SKDB en uit deze databank gegevens ontvangen, gebruiken in hun primaire (strafrechtelijke) processen de set van gegevens die in de SKDB bij het desbetreffende SKN als leidend is aangemerkt (de "Leidende Administratieve Identiteit", LAI). Wanneer zij de desbetreffende gegevens overnemen of hebben overgenomen in hun eigen bestanden, volgen zij het oordeel van de Matching Autoriteit en passen zij hun bestanden aan. Dit kan geautomatiseerd dan wel handmatig worden gedaan. Iedere ketenpartner stelt hiervoor procedures op en wijst functionarissen aan die bevoegd zijn de eventuele aanpassingen door te voeren in de bestanden. De oorspronkelijke, afwijkende gegevens worden in de SKDB voor de historie bewaard.

Op basis van de als leidend aangemerkte gegevens worden documenten aangemaakt, zoals processen-verbaal, brieven, vorderingen, bevelen, aktes, oproepingen, beschikkingen, vonnissen.[25] Nadat een dergelijk document is opgesteld en ondertekend, gaat het zijn functie vervullen in het primaire proces: het proces-verbaal wordt ingezonden naar de officier van justitie, de dagvaarding wordt betekend, de brief toegezonden, enz.. Zo'n document kan dan niet meer worden veranderd, ook al wordt nadien - op basis van nadere en eventueel betere informatie - een andere set van gegevens als leidend aangemerkt. Deze stand van zaken kan ertoe leiden dat op verschillende documenten in hetzelfde traject verschillende personalia komen te staan. Iedere functionaris die toegang heeft tot de SKDB zal in die databank de historie van de set van gegevens kunnen raadplegen. Daarmee kunnen onduidelijkheden en misverstanden binnen de keten worden voorkomen. Naar de justitiabele toe kan wellicht misverstand worden voorkomen doordat aan latere documenten zo nodig informatie wordt toegevoegd waaruit blijkt dat (en eventueel ook waarom of op basis waarvan) het latere document andere personalia bevat dan eerdere documenten. Bijvoorbeeld kunnen in documenten aan de personalia clausuleringen worden toegevoegd zoals: "zich noemende", "ook wel bekend als", "eerder aangeduid als", en dergelijke.
Sluitstuk van het stelsel van afspraken is dat geen enkele partij of functionaris in de keten zelfstandig personalia van verdachten of veroordeelden in (eigen of gezamenlijke) bestanden wijzigt buiten de Matching Autoriteit om. De betrokken

[25] De artikelen 588 en 588a van het Wetboek van Strafvordering bevatten bijzondere regels voor de gegevens op basis waarvan een gerechtelijke mededeling moet worden uitgereikt resp. een afschrift van de dagvaarding of oproeping van de verdachte om op de terechtzitting of nadere terechtzitting te verschijnen moet worden toegezonden.

organisaties verankeren dit op beveiligingstechnisch niveau. Dit wil zeggen dat zij de mogelijkheid voor het aanbrengen van wijzigingen uitsluiten of beperken voor de lokale gebruikers. Voor het doorvoeren van wijzigingen door de Justitiële Informatiedienst zelf geldt het "vier-ogen principe". Dit wil zeggen dat wijzigingen niet door één medewerker alleen kunnen worden doorgevoerd. Alle bewerkingen worden gelogd. De dossiers worden steekproefsgewijs gecontroleerd door een senior-medewerker. De loggingbestanden worden periodiek gecontroleerd door een leidinggevende.

GEBRUIKTE AFKORTINGEN

Bivv Besluit identiteitsvaststelling verdachten en veroordeelden
BOA buitengewoon opsporingsambtenaar
BOD bijzondere opsporingsdienst
BRP
BSN
Basisregistratie Personen
burgerservicenummer
BVV Basisvoorziening Vreemdelingen
CJIB Centraal Justitieel Incassobureau
DGRR Directoraat-Generaal Rechtspleging en Rechtshandhaving
DJI Dienst Justitiële Inrichtingen
DRM
EEGG
Directie Regie Migratieketen
echt, eigen, geldig en gekwalificeerd
GGZ geestelijke gezondheidszorg
IND Immigratie- en Naturalisatiedienst
KMar Koninklijke Marechaussee
LAI leidende administratieve identiteit
MA Matching Autoriteit
NFI Nederlands Forensisch Instituut
NIFP Nederlands Instituut voor Forensisch Psychiatrie en Psychologie
OM Openbaar Ministerie
OvJ officier van justitie
PI penitentiaire inrichting
RDW Dienst voor het Wegverkeer
RNI Register Niet-Ingezetenen
3RO de drie reclasseringsinstellingen
SKDB strafrechtsketendatabank
SKN strafrechtsketennummer
VH voorlopige hechtenis
VRIS (Protocol) vreemdeling in de strafrechtsketen
WID Wet op de identificatieplicht
Wivvg Wet identiteitsvaststelling verdachten, veroordeelden en getuigen

WvSv Wetboek van Strafvordering

Voor akkoord:

Yvonne Hondema,
Politiechef Midden-Nederland

16-10-2024

Bron	Risico analyse / GEB (documentnaam)	Portefeuille volgens Priv. Prg.	Verwerking volgens Priv. Prg.	Thema	Mission Critical System	Top-8 risico	BIV Aspect B	I	V	Risicoscore (Kans x Impact)			Risicoclassificatie	Risico omschrijving	Geadviseerde Maatregel(en)	Maatregelcategorie (keyword inschatting)	Datum aanvoer maatregel (baseline: 01-01-2024)	Actiehouder	Datum gepland gereed
Privacy	20211214 PRA Toezicht BOA.xlsx	GGP	Toezicht houden (algemeen)	Rechtmatigheid			x			4	3	12	Hoog	Als de grondslag ontbreekt dan is de verwerking mogelijk niet rechtmatig waardoor gestopt moet worden met de verwerking.	Advies is om het ingezette overleg met J&V en OM te concretiseren en de voorstellen in uitvoering te nemen zodat er een expliciete grondslag is voor de continue toetsing van betrouwbaarheid van (aspirant) Boa's. Indien dit geen concreet resultaat oplevert is het advies dit te overleggen met de FG.	IB risico	1-1-2024		
Privacy	20211214 PRA Toezicht BOA.xlsx	GGP	Toezicht houden (algemeen)	Rechtmatigheid				x	x	3	3	9	Midden	Als bewaartermijnen niet zijn bepaald, niet worden nageleefd dan worden gegevens mogelijk te lang bewaard waardoor deze gebruikt kunnen worden voor andere dan de oorspronkelijke doeleinden, meer kans op dataverlies, schending van vertrouwelijkheid.	Advies is aansluiting te zoeken bij gelijksoortige processen die wel zijn opgenomen in de selectielijst , zoals 2.04.06 (het verlenen, intrekken en verlengen van vergunningen in het kader van bestuurlijke korpscheftaken) en 2.04.07 (het adviseren met betrekking tot vergunningsverlening, intrekking en verlenging door derden). Verder kan 3.02.01 (Het ontwikkelen, evalueren en begeleiden van personeel) relevant zijn. Verder zal er een archiverings- of verwijderinstructie moeten worden geïmplementeerd. Dit zal in de nieuwe Boa module in Verona moeten worden ingeregeld	IB risico	1-1-2024		
Privacy	20211214 PRA Toezicht BOA.xlsx	GGP	Toezicht houden (algemeen)	Processen, procedures				x	x	3	3	9	Midden	Als de processen niet actueel en of overzichtelijk zijn dan leidt dat eerder tot fouten waardoor de kwaliteit of de vertrouwelijkheden rechtmatigheid niet geborgd zijn.	De PSH-VM omgeving (Politie suite handhaving – Vergunning module) wordt uitgebreid met een Boa omgeving. Dit is een uitgelezen mogelijkheid om de processen te uniformeren en zaken als bewaartermijnen en data minimalisatie in te regelen.	IB risico	1-1-2024		
Privacy	20211214 PRA Toezicht BOA.xlsx	GGP	Toezicht houden (algemeen)	Kennis					x	2	2	4	Midden	Als het bewustzijnsniveau onvoldoende is dan is er meer kans op onrechtmatige verwerking van persoonsgegevens waardoor mogelijk schending van vertrouwelijkheid plaatsvindt.	Het advies is om de bewustwordingstrainingen van de politie aantoonbaar te volgen en eventueel periodiek te herhalen.	IB risico	1-1-2024		
Privacy	20211214 PRA Toezicht BOA.xlsx	GGP	Toezicht houden (algemeen)	Rechten van betrokken			x		x	3	3	9	Midden	Als de betrokkene niet geïnformeerd is (bij een grondslag zoals toestemming) dan kan deze mogelijk zijn rechten niet uitoefenen waardoor de betrokkene de grip op het gebruik van zijn persoonsgegevens verliest	Om hierin te voorzien is een afzonderlijk privacy statement opgesteld voor verwerkingen die voortvloeien uit de korpscheftaken, waaronder het direct toezichthouderschap op de Boa's. Daarnaast wordt er gewerkt aan een informatiebrochure die bij elke eerste verwerking aan betrokkenen wordt uitgereikt.	IB risico	1-1-2024		
Privacy	20211214 PRA Toezicht BOA.xlsx	GGP	Toezicht houden (algemeen)	Bijzondere gegevens			x			3	3	9	Midden	Als strafrechtelijke gegevens worden verwerkt zonder de juiste rechtvaardigingsgrondslag dan is dat onrechtmatig en is er een verhoogd risico op oneigenlijk gebruik en nadelige gevolgen voor de betrokkene zoals uitsluiting, discriminatie of stigmatisering.	[invullen]	IB risico	1-1-2024		
Privacy	20230703 WPG GEB Uitvoeren Rechtbanktaken_vs 1.0_DEF.pdf	Arrestantentaken	Rechtbanktaken	Verwerkings-verantwoordelijke				x	x	5	3	15	Hoog	Issue: Er is op structurele basis geen duidelijke product-owner en beheerder van het Registratiesysteem Parkettaken. Risico: (i) de verantwoordelijkheid voor zaken als het bewaken van verwerkings-en bewaartermijnen, het toezien op security-issues, het oplossen van incidenten, het voorkomen van datalekken etc. is niet voldoende belegd, waardoor privacy-en security incidenten kunnen ontstaan (ii) de rechten van betrokkenen kunnen niet worden uitgeoefend.	De portefeuillehouder benoemt een product-owner en beheerder voor het Registratiesysteem Parketaken.	IB risico	1-1-2024		
Privacy	20230703 WPG GEB Uitvoeren Rechtbanktaken_vs 1.0_DEF.pdf	Arrestantentaken	Rechtbanktaken	Privacy beleid			x	x	x	4	4	16	Hoog	Issue: de verwerking is in strijd met wettelijke eisen en de privacy vereisten van het interne beleid (Beleidskader logging, Uitvoeringskader privacy & security by design, Informatiebeveiligingsbeleid). Risico: (i) datalekken	Pas de verwerking aan conform het beleid en geef instructies aan de betreffende functionaris(sen). Pas privacy by design en default toe om efficiency en privacybescherming te bereiken en om aan de Wpg te voldoen.	Werkproces gerelateerd	1-1-2024		
Privacy	20230703 WPG GEB Uitvoeren Rechtbanktaken_vs 1.0_DEF.pdf	Arrestantentaken	Rechtbanktaken	Werkproces						4	1	4	Midden	Issue: De verwerking heeft een verouderd werkproces in de bedrijfsarchitectuur. Risico: o.a. de verwerking is niet transparant	Zorg dat de werkprocessen geactualiseerd worden, centraal vastgesteld zijn en beschikbaar zijn gesteld	Werkproces gerelateerd	1-1-2024		
Privacy	20230703 WPG GEB Uitvoeren Rechtbanktaken_vs 1.0_DEF.pdf	Arrestantentaken	Rechtbanktaken	Uitvoering					x	3	3	9	Midden	Issue: De verwerking wordt in de eenheden niet uniform uitgevoerd. Risico: de verwerking is niet transparant; ongelijke behandeling van arrestanten voor zover het de verwerking van hun persoonsgegevens betreft	Stel landelijke richtlijnen en protocollen over de gegevensverwerking in relatie tot rechtbanktaken op en controleer deze regelmatig (ook in Amsterdam, Rotterdam en Den Haag).	IB risico	1-1-2024		
Privacy	20230703 WPG GEB Uitvoeren Rechtbanktaken_vs 1.0_DEF.pdf	Arrestantentaken	Rechtbanktaken	Autorisatie					x	5	4	20	Zeer hoog	Issue: [redacted] Autorisaties worden niet periodiek gecontroleerd. Risico: [redacted]	[redacted] Controleer de autorisaties regelmatig [redacted]	IB risico	1-1-2024		
Privacy	20230703 WPG GEB Uitvoeren Rechtbanktaken_vs 1.0_DEF.pdf	Arrestantentaken	Rechtbanktaken	Verwerkingstermijnen Bewaartermijnen				x		5	3	15	Hoog	Issue: De verwerkingstermijnen en bewaartermijnen worden niet nageleefd, waardoor de verwerking langer plaatsvindt en de gegevens langer toegankelijk zijn dan wettelijk is toegestaan. Risico: o.a. onrechtmatige gegevensverwerking.	Pas systemen en procedures aan om de verwerkingstermijnen en bewaartermijnen na te leven.	IB risico	1-1-2024		
Privacy	20230703 WPG GEB Uitvoeren Rechtbanktaken_vs 1.0_DEF.pdf	Arrestantentaken	Rechtbanktaken	Kennis					x	3	3	9	Midden	Issue: Het bouwteam van het Registratiesysteem Rechtbanktaken blijkt niet of onvoldoende op de hoogte van de privacyregels. Risico: o.a. datalekken, geen toepassing van de principes van privacy en security by design.	Geef regelmatig privacy training. Denk hierbij aan het volgen van een training op het gebied van privacy awareness, meer in het bijzonder op het gebied van privacy en security by design.	IB risico	1-1-2024		
Privacy	20230703 WPG GEB Uitvoeren Rechtbanktaken_vs 1.0_DEF.pdf	Arrestantentaken	Rechtbanktaken	Overige risico's mens					x	4	3	12	Hoog	Issue: er zijn vanuit de portefeuille geen richtlijnen/werkinstructies opgesteld om de uitoefening van de rechten van betrokkenen af te stemmen op de processen van de privacy desks waar de verzoeken van betrokkenen binnenkomen Risico: onvermogen om de juiste informatie te vinden om aan inzageverzoeken en verzoeken tot rectificatie en vernietiging te voldoen; overschrijding van termijnen voor de uitoefening van de rechten van betrokkenen	Richt een proces in voor inzageverzoeken.	IB risico	1-1-2024		

Privacy	20230703 WPG GEB Uitvoeren Rechtbanktaken_vs 1.0_DEF.pdf	Arrestantentaken	Rechtbanktaken	Bijzonder persoonsgegevens					x	4	5	20	Zeer hoog	Issue: er ontbreken concrete werkinstructies over de omgang met bijzondere persoonsgegevens in het kader van deze verwerking. Risico: onwettige verwerking, arrestant wordt aangetast in zijn persoonlijke levenssfeer	Stel heldere werkinstructies op en instrueer de collega's werkzaam bij de gerechten over deze werkinstructies	Werkproces gerelateerd	1-1-2024
Privacy	20230703 WPG GEB Uitvoeren Rechtbanktaken_vs 1.0_DEF.pdf	Arrestantentaken	Rechtbanktaken	Logging					x	5	4	20	Zeer hoog	Issue: Het Registratiesysteem Parkettaken logged niet. Risico: o.a. datalekken door niet te traceren onrechtmatige toegang tot gegevens	Richt logging in gebaseerd op instructies van de GA (Beleidskader Logging)	Werkproces gerelateerd	1-1-2024
Privacy	20230703 WPG GEB Uitvoeren Rechtbanktaken_vs 1.0_DEF.pdf	Arrestantentaken	Rechtbanktaken	Gegevensverstrekking			x			5	1	5	Midden	Issue: grondslag gegevensverstrekking aan rechtbank/hoven is niet duidelijk Risico: onrechtmatige gegevensverwerking	Nader juridisch onderzoek en interne juridische afstemming zou plaats kunnen vinden om te bepalen of hiervoor in het Bpg een voorziening zou moeten worden getroffen. Bij die afweging zal echter de beperkte impact van dit issue meegewogen moeten worden.	IB risico	1-1-2024
Privacy	20230831 GEB VIK Klachten_versie 1.0_DEF.pdf	VIK	VIK-Klachten	Autorisaties					x	4	5	20	Zeer hoog	Issue: 5.1.2.i Risico: 5.1.2.i	5.1.2.i en voor reguliere controle van de autorisaties volgens 5.1.2.i	Werkproces gerelateerd	1-1-2024
Privacy	20230831 GEB VIK Klachten_versie 1.0_DEF.pdf	VIK	VIK-Klachten	Autorisaties					x	4	5	20	Zeer hoog	Issue: 5.1.2.i Risico: 5.1.2.i	5.1.2.i	IB risico	1-1-2024
Privacy	20230831 GEB VIK Klachten_versie 1.0_DEF.pdf	VIK	VIK-Klachten	Autorisaties					x	4	5	20	Zeer hoog	Issue: 5.1.2.i Risico: 5.1.2.i	5.1.2.i	IB risico	1-1-2024
Privacy	20230831 GEB VIK Klachten_versie 1.0_DEF.pdf	VIK	VIK-Klachten	Bewaartermijnen				x		4	3	12	Hoog	Issue: Bewaartermijn is wel bepaald, maar er wordt niet naar gehandeld. Risico: De verwerking vindt langer plaats dan is toegestaan, langer inbreuk op de privacy van betrokkene.	Documentum aanpassen zodat klachtdossiers worden verwijderd na het verstrijken van de bewaartermijn en stoppen met het uitprinten en fysiek bewaren van dossiers.	IB risico	1-1-2024
Privacy	20230831 GEB VIK Klachten_versie 1.0_DEF.pdf	VIK	VIK-Klachten	Rechten van betrokkenen					x	4	3	12	Hoog	Issue: De betrokkene wordt niet volledig geïnformeerd conform de eisen van de AVG. De betrokkene kan de informatie niet makkelijk vinden. Documenten zijn gericht op informatie over het klachtenproces en niet op de verwerking van persoonsgegevens binnen het klachtenproces. Risico: Betrokkene kan zijn rechten zoals inzage en rectificatie niet uitoefenen, omdat hij/zij geen weet heeft dat of in welke mate persoonsgegevens over hem/haar worden verwerkt.	Werk de brochure Niet tevreden over de politie? en de brochure Een klacht. Wat nu? bij en beschrijf daarin specifieker welke (categorieën) persoonsgegevens worden verwerkt. Geef daarbij ook specifiek aan waar de toepasselijke privacy statements op intranet/ internet kunnen worden gevonden.	IB risico	1-1-2024
Privacy	20230831 GEB VIK Klachten_versie 1.0_DEF.pdf	VIK	VIK-Klachten	Kennis				x		2	4	8	Midden	Issue: De klachtbehandelaren zijn mogelijk onvoldoende op de hoogte van de privacyregels. Risico: Mogelijke onjuiste gegevensverwerking.	Geef regelmatig zoveel mogelijk op de verwerking gerichte privacy training.	IB risico	1-1-2024
Privacy	20230831 GEB VIK Klachten_versie 1.0_DEF.pdf	VIK	VIK-Klachten	Noodzakelijkheid/ Proportionaliteit					x	4	5	20	Zeer hoog	Issue: De klachtbehandelaar heeft de mogelijkheid een veelheid aan gegevens te verwerken, zonder dat er duidelijke beleidslijnen zijn die richting geven welke gegevens in welke gevallen geraadpleegd en verder verwerkt mogen worden. Er worden hierdoor naar verwachting meer gegevens verwerkt dan redelijkerwijs noodzakelijk is Risico: onrechtmatige gegevensverwerking, meer inbreuk op de privacy dan redelijkerwijs noodzakelijk is, misbruik van gegevens en datalekken.	Maak klacht-behandelaren bewust dat zij alleen gegevens mogen verwerken als dat noodzakelijk is om een klacht af te kunnen handelen. Bepaal welke gegevens noodzakelijk zijn voor het afhandelen van klachten en verwerkt mogen worden. Geef tevens aan welke gegevens niet verwerkt mogen worden.	IB risico	1-1-2024
Privacy	20230831 GEB VIK Klachten_versie 1.0_DEF.pdf	VIK	VIK-Klachten	Bijzondere persoonsgegevens					x	4	5	20	Zeer hoog	Issue: Sommige klachtbehandelaren delen incidenteel persoonsgegevens van klagers met onbegrepen gedrag uit serviceoverweging met zorginstellingen en de zorgcoördinator van een basisteam. Daarnaast worden er ook bijzondere persoonsgegevens verwerkt waarvan het gebruik te vermijden is en daarmee dus niet aan het evidentie criterium is voldaan. Risico: Onrechtmatige gegevensverwerking.	Stoppen met delen van deze persoonsgegeven.	IB risico	1-1-2024
Privacy	20230831 GEB VIK Klachten_versie 1.0_DEF.pdf	VIK	VIK-Klachten	5.1.2.i				x	x	4	5	20	Zeer hoog	Issue: 5.1.2.i Risico: 5.1.2.i	5.1.2.i 5.1.2.i	IB risico	1-1-2024

Privacy	20230831 GEB VIK Klachten_versie 1.0_DEF.pdf	VIK	VIK-Klachten	Opslag van gegevens			x	x	x	4	3	12	Hoog	Issue: Er worden naast het klachtdossier in Documentum ook dossiers op netwerkschijven gevormd. Ook worden dossiers uitgeprint en fysiek in kasten bewaard. Uit het onderzoek is geen volledig beeld verkregen van hoe het klachtenformulier vanaf de website van de politie wordt overgezet naar Documentum, of de inhoud van het klachtenformulier nog op andere plaatsen dan Documentum wordt opgeslagen, of hierbij de bewaartermijnen worden gehanteerd en wie toegang tot de informatie heeft. Risico: Niet in control zijn waar documenten zich bevinden (schaduwdossier). Documenten zouden kunnen gaan “rondslingeren” en langer worden bewaard dan toegestaan. Hierdoor neemt de kans toe op incidenten met betrekking tot de beschikbaarheid, integriteit of vertrouwelijkheid van persoonsgegevens.	Maak duidelijke afspraken over waar dossiers worden opgeslagen. Verricht nader onderzoek over hoe het klachtenformu-lier vanaf de website van de politie wordt overgezet naar Documentum, of de inhoud van het klachtenformulier nog op andere plaatsen dan Documentum wordt opgeslagen, of hierbij de bewaartermijn-en worden gehanteerd en wie toegang tot de informatie heeft.	IB risico	1-1-2024
Privacy	20230918 Dienstverlening - GEB Intake - versie 1.0.pdf	Dienstverlening	Intake	Werkproces						4	1	4	Midden	Issue: De verwerking heeft een verouderd werkproces in de bedrijfsarchitectuur. Risico: De verwerking is niet transparant en onvoldoende beheersbaar.	Zorg dat de werkprocessen geactualiseerd worden in de bedrijfsarchitectuur, centraal vastgesteld zijn en beschikbaar zijn gesteld.	Werkproces gerelateerd	1-1-2024
Privacy	20230918 Dienstverlening - GEB Intake - versie 1.0.pdf	Dienstverlening	Intake	Uitvoering						2	3	6	Midden	Issue: De verwerking wordt in de eenheden nog niet uniform uitgevoerd. Risico: ongelijke behandeling van burgers voor zover het de verwerking van hun politiegegevens betreft.	Bepaal een landelijke werkwijze voor de gegevensverwerking in relatie tot het intake-proces en controleer deze op regelmatige basis.	IB risico	1-1-2024
Privacy	20230918 Dienstverlening - GEB Intake - versie 1.0.pdf	Dienstverlening	Intake	Autorisatie					x	3	4	12	Hoog	Issue: 5.1.2.i . Autorisaties worden niet periodiek gecontroleerd. Risico: 5.1.2.i	Beperk en controleer de autorisaties regelmatig 5.1.2.i	IB risico	1-1-2024
Privacy	20230918 Dienstverlening - GEB Intake - versie 1.0.pdf	Dienstverlening	Intake	Verwerkingstermijnen Bewaartermijnen						4	4	16	Hoog	Issue: De verwerkingstermijnen en vernietigingstermijnen worden slechts gedeeltelijk nageleefd, waardoor sommige verwerkingen langer plaatsvinden en de gegevens langer toegankelijk zijn dan wettelijk is toegestaan. De verwerkingstermijnen en vernietigingstermijnen van e-mail (outlook) en de downloads vanuit BVH 5.1.2.i zijn onvoldoende inzichtelijk. Deze blijven in de map of postvakken staan en worden niet verwijderd of vernietigd. Risico: o.a. onrechtmatige gegevensverwerking.	Stel een policy in voor het periodiek schonen 5.1.2.i Onderzoek of/welke oplossing mogelijk is voor het naleven van de verwerkings-en vernietigingstermijnen voor gegevens in Outlook.	IB risico	1-1-2024
Privacy	20230918 Dienstverlening - GEB Intake - versie 1.0.pdf	Dienstverlening	Intake	Datakwaliteit				x		3	4	12	Hoog	Issue: De kwaliteit van de gegevens in de Service Module wordt niet gecontroleerd of is niet voldoende (juistheid, volledigheid, controle op dubbele invoer). Risico: dubbele en/of onjuiste politiegegevens in de Service Module.	Richt een kwaliteitstoets in waarbij regelmatig datakwaliteit wordt getoetst. Denk hierbij aan een interne controle waarbij steekproeven worden gehouden op de kwaliteit van de ingevoerde gegevens. Wellicht kan hierbij een reminder in het systeem worden ingebouwd. Denk hier ook aan het volgen van een privacy training.	IB risico	1-1-2024
Privacy	20230918 Dienstverlening - GEB Intake - versie 1.0.pdf	Dienstverlening	Intake	Bijzondere Persoonsgegevens						3	3	9	Midden	Issue: door opname van alle gesprekken worden naar verwachting ook bijzondere politiegegevens opgenomen die strikt genomen niet noodzakelijk zijn volgens de criteria van art. 5 Wpg Risico: onrechtmatige verwerking van bijzondere politiegegevens Issue: er is geen rechtsgrondslag om politiegegevens te verstrekken voor coachingsdoeleinden (“van Wpg naar AVG”)	Issue is lastig op te lossen, omdat er wel valide gronden zijn om alle gesprekken op te nemen (met name opsporingsbelang). Risico’s worden al gemitigeerd, omdat deze gegevens beperkt toegankelijk zijn en het protocol ‘Monitoring RSC’ voorziet in spelregels voor verstrekking.	IB risico	1-1-2024
Privacy	20230918 Dienstverlening - GEB Intake - versie 1.0.pdf	Dienstverlening	Intake	Overig			x			3	3	9	Midden	Risico: Voor het verstrekken van gesprekken in het kader van coachingsdoeleinden is er formeel op dit moment geen rechtsgrondslag. Hierdoor bestaat het risico dat de informatie onwettig verstrekt is.	De meest vergaande maatregel is om de gesprekken niet terug te luisteren voor coachingsdoelen, maar de vraag is of dit wenselijk is. Het risico wordt op dit moment gemitigeerd, omdat waarborgen zijn ingebouwd in het protocol ‘Monitoring RSC’. Strikt genomen zou er in de toekomst in een juridische verstrekkingsgrondslag moeten worden voorzien.	IB risico	1-1-2024
Privacy	20230918 Dienstverlening - GEB Intake - versie 1.0.pdf	Dienstverlening	Intake	Overig			x	x	x	3	3	9	Midden	Issue: De gesprekken worden allemaal opgenomen. Hier is een protocol voor opgesteld ‘Monitoring RSC’. Risico: Het risico bestaat dat als het protocol niet strikt wordt uitgevoerd er te veel gesprekken worden verstrekt of ter beschikking worden gesteld aan andere afdelingen.	Het protocol ‘monitoring RSC’ bestaat uit regels wanneer een opname van een gesprek wel of niet wordt verstrekt. Deze regels zijn per onderwerp klachten, coaching of opsporingsonderzoek vastgesteld. De regels zijn zorgvuldig samengesteld op een aanvraagformulier dat ingevuld en goedgekeurd dient te worden. Zorg ervoor dat het protocol in de praktijk goed worden uitgevoerd en dat het up to date blijft.	IB risico	1-1-2024
Privacy	20230918 Dienstverlening - GEB Intake - versie 1.0.pdf	Dienstverlening	Intake	Regime						4	1	4	Midden	Issue: In deze GEB zijn we, zoals uitgelegd in punt 1.2, uitgegaan van het WPG-regime. Binnen deze verwerking vindt echter ook een klein deel AVG-verwerkingen plaats. Risico: Mogelijk zijn er andere bevindingen bij de toetsing van de AVG-verwerkingen.	Er kan een aanvullende GEB uitgevoerd worden op het (kleine) deel AVG-verwerkingen binnen het Intakeproces.	IB risico	1-1-2024
Privacy	20231026 GEB_AVG_Oriënterend Onderzoek_1.0_DEF.pdf	VIK	VIK - Intern onderzoek-oriënterend	Autorisaties					x	4	5	20	Zeer hoog	Issue: 5.1.2.i Risico: 5.1.2.i	5.1.2.i . Zorg voor reguliere controle van de autorisaties volgens het beleid 5.1.2.i	Werkproces gerelateerd	1-1-2024

Privacy	20231026 GEB_AVG_Oriënterend Onderzoek_1.0_DEF.pdf	VIK	VIK - Intern onderzoek-oriënterend	Autorisaties					x	4	5	20	Zeer hoog	Issue: 5.1.2.i Risico: 5.1.2.i	5.1.2.i	IB risico	1-1-2024
Privacy	20231026 GEB_AVG_Oriënterend Onderzoek_1.0_DEF.pdf	VIK	VIK - Intern onderzoek-oriënterend	Autorisaties					x	3	5	15	Hoog	Issue: 5.1.2.i Risico: 5.1.2.i	Geef hierover trainingen en controleer het gebruik van autorisaties.	IB risico	1-1-2024
Privacy	20231026 GEB_AVG_Oriënterend Onderzoek_1.0_DEF.pdf	VIK	VIK - Intern onderzoek-oriënterend	Bewaartermijnen				x		4	3	12	Hoog	Issue: 5.1.2.i Risico: De verwerking vindt langer plaats dan is toegestaan.	Regel beleid en werkprocessen in om de bewaartermijnen gestand te doen.	Werkproces gerelateerd	1-1-2024
Privacy	20231026 GEB_AVG_Oriënterend Onderzoek_1.0_DEF.pdf	VIK	VIK - Intern onderzoek-oriënterend	Bewaartermijnen					x	4	3	12	Hoog	Issue: Persoonsgegevens die voor het onderzoek zijn verzameld, maar waarvan na analyse is gebleken dat ze niet relevant blijken voor het onderzoek, worden te lang bewaard. Risico: De verwerking vindt langer plaats dan is toegestaan.	Vanuit AVG-perspectief moeten deze persoonsgegevens worden vernietigd, althans onleesbaar worden gemaakt. Vanuit het VIK werd voorts als mogelijke maatregel geopperd dit risico te beperken door in ieder geval de loggegevens uitsluitend bij het FDO te bewaren en niet tevens bij de VIKs.	IB risico	1-1-2024
Privacy	20231026 GEB_AVG_Oriënterend Onderzoek_1.0_DEF.pdf	VIK	VIK - Intern onderzoek-oriënterend	Rechten van betrokkenen					x	4	3	12	Hoog	Issue: De betrokkenen worden niet volledig geïnformeerd conform de eisen van de AVG. De betrokkenen kunnen de informatie niet makkelijk vinden. Risico: Betrokkenen kunnen hun rechten zoals inzage en rectificatie niet uitoefenen, omdat zij geen weet hebben dat of in welke mate persoonsgegevens over hen worden verwerkt.	Neem bij de aanpassingen van de Brochure Intern Onderzoek de informatieverplichtingen uit de AVG mee en beschrijf daarin welke (categorieën) persoonsgegevens worden verwerkt. Geef daarbij ook specifiek aan waar de toepasselijke privacy informatie op intranet / internet kan worden gevonden. Zorg er ook voor dat burgergetuigen conform de regels van de AVG worden geïnformeerd over hoe er met hun gegevens wordt omgegaan. Dit kan bijvoorbeeld door uitreiking van een flyer met de noodzakelijke informatie.	IB risico	1-1-2024
Privacy	20231026 GEB_AVG_Oriënterend Onderzoek_1.0_DEF.pdf	VIK	VIK - Intern onderzoek-oriënterend	Er is te weinig privacy ondersteuning voor het VIK				x		3	3	9	Midden	Issue: Functionarissen kunnen niet altijd terecht bij een privacy adviseur met kennis van zaken van specifieke VIK gerelateerde privacyvraagstukken. Risico: Mogelijke onjuiste gegevensverwerking	Wijs een privacy adviseur aan met kennis van de VIK-processen die de VIKs kan ondersteunen.	IB risico	1-1-2024
Privacy	20231026 GEB_AVG_Oriënterend Onderzoek_1.0_DEF.pdf	VIK	VIK - Intern onderzoek-oriënterend	Kennis				x		2	4	8	Midden	Issue: De functionarissen zijn mogelijk onvoldoende op de hoogte van de privacy regels. Risico: Mogelijke onjuiste gegevensverwerking	Geef regelmatig zoveel mogelijk op de verwerking gerichte privacy training.	IB risico	1-1-2024
Privacy	20231026 GEB_AVG_Oriënterend Onderzoek_1.0_DEF.pdf	VIK	VIK - Intern onderzoek-oriënterend	Discipline					x	3	3	9	Midden	Issue: Voor een uniforme werkwijze is het essentieel dat alle VIK-onderzoekers zich aan de gemaakte werkafspraken houden. Het is onzeker of dit voldoende gebeurt. Risico: Het risico bestaat dat de verwerking van persoonsgegevens niet conform de AVG geschiedt en de betrokkenen niet de bescherming hebben die de AVG aan hen biedt. Verder worden betrokkenen -medewerkers die onderwerp zijn van een oriënterend onderzoek-mogelijk ongelijk behandeld, als de aanpak van eenheden in de praktijk onvoldoende uniform is.	Teamchefs en coördinatoren moeten sturing geven zodanig dat de VIK-onderzoekers conform de werkafspraken werken (cultuurkwestie) Verricht steekproeven.	IB risico	1-1-2024
Privacy	20231026 GEB_AVG_Oriënterend Onderzoek_1.0_DEF.pdf	VIK	VIK - Intern onderzoek-oriënterend	5.1.2.i						2	5	10	Hoog	Issue: 5.1.2.i Risico: 5.1.2.i	5.1.2.i 5.1.2.i	IB risico	1-1-2024

Privacy	20231026 GEB_AVG_Oriënterend Onderzoek_1.0_DEF.pdf	VIK	VIK - Intern onderzoek-oriënterend	Proportionaliteit en subsidiariteit					x	4	5	20	Zeer hoog	Issue: 5.1.2.i Risico: 5.1.2.i	AVG-toets van de inzet van onderzoeksmiddelen inbedden, door te allen tijde advies in te winnen bij een privacy adviseur. 5.1.2.i Een duidelijk overzicht opstellen welke bronnen (applicaties / systemen) mogen worden geraadpleegd. Evaluatie om te bepalen of de inzet van de onderzoeksmiddelen achteraf gezien proportioneel was. Doorvoeren van verbeterpunten n.a.v. evaluaties.	Werkproces gerelateerd	1-1-2024
Privacy	20231026 GEB_AVG_Oriënterend Onderzoek_1.0_DEF.pdf	VIK	VIK - Intern onderzoek-oriënterend	Proportionaliteit en subsidiariteit					x	3	4	12	Hoog	Issue: Er worden audio opnames gemaakt van de gesprekken met de betrokkene en/ of getuige. Dit gebeurt echter slechts incidenteel. Risico: Er worden mogelijk meer persoonsgegevens verwerkt dan noodzakelijk; er worden mogelijk bijzondere persoonsgegevens verwerkt zonder dat daar een uitzonderingsgrond voor is.	Stop met de audio opnames, tenzij de audio opname plaatsvindt op verzoek van de betrokkene.	IB risico	1-1-2024
Privacy	20231026 GEB_AVG_Oriënterend Onderzoek_1.0_DEF.pdf	VIK	VIK - Intern onderzoek-oriënterend	Bijzondere persoonsgegevens-uit hoorgesprek				x	x	3	4	12	Hoog	Issue: Er is geen wettelijke uitzondering voor: Bijzondere persoonsgegevens die: (i) medegedeeld zijn tijdens hoorgesprekken; én (ii) zijn vastgelegd (bijv. schriftelijk of elektronisch in een verslag of door middel van gespreksopname); én (iii) die niet noodzakelijk zijn ten behoeve van het onderzoek omdat niet aan het evidentie criterium is voldaan. Risico: Als deze gegevens worden gebruikt in het kader van oriënterende onderzoeken, gebeurt dit in strijd met de AVG. Juist bijzondere persoonsgegevens worden extra beschermd in de AVG gezien hun gevoelige aard, dus schending van deze regels heeft een nadelige impact op de persoonlijke levenssfeer van een betrokkene.	Medewerkers instrueren zeer kritisch te zijn met het vermelden van bijzondere persoonsgegevens in de hoorverslagen. Als opname van gesprekken achterwege wordt gelaten, is er geen risico dat ten onrechte bijzondere persoonsgegevens "op band" komen te staan.	IB risico	1-1-2024
Privacy	20231026 GEB_AVG_Oriënterend Onderzoek_1.0_DEF.pdf	VIK	VIK - Intern onderzoek-oriënterend	Bijzondere persoonsgegevens – open bronnen					x	3	4	12	Hoog	Issue: Er is geen wettelijke uitzondering: Bijzondere persoonsgegevens ontleend aan open bronnen die niet door een betrokkene zelf zijn openbaar gemaakt. Risico: Als deze gegevens worden gebruikt in het kader van oriënterende onderzoeken, gebeurt dit in strijd met de AVG. Juist bijzondere persoonsgegevens worden extra beschermd in de AVG gezien hun gevoelige aard, dus schending van deze regels heeft een nadelige impact op de persoonlijke levenssfeer van een betrokkene.	Medewerkers instrueren zeer kritisch te zijn met het verzamelen van bijzondere persoonsgegevens uit open bronnen als het gaat om bijzondere persoonsgegevens die niet door een betrokkene zelf zijn openbaar gemaakt.	IB risico	1-1-2024
Privacy	20231026 GEB_AVG_Oriënterend Onderzoek_1.0_DEF.pdf	VIK	VIK - Intern onderzoek-oriënterend	Bijzondere persoonsgegevens – ontleend aan politiesystemen ("bijvangst")					x	3	4	12	Hoog	Issue: Er is geen wettelijke uitzondering: Bijzondere persoonsgegevens die onderdeel zijn van gegevens verkregen uit de politiesystemen ("bijvangst") én die niet voldoen aan de criteria van artikel 23 sub c UAVG (verwerking noodzakelijk in aanvulling op verwerking strafrechtelijke gegevens). Risico: Als deze gegevens worden gebruikt in het kader van oriënterende onderzoeken, gebeurt dit in strijd met de AVG. Juist bijzondere persoonsgegevens worden extra beschermd in de AVG gezien hun gevoelige aard, dus schending van deze regels heeft een nadelige impact op de persoonlijke levenssfeer van een betrokkene.	Medewerkers instrueren zeer kritisch te zijn met het verzamelen van bijzondere persoonsgegevens.	IB risico	1-1-2024
Privacy	20231026 GEB_AVG_Oriënterend Onderzoek_1.0_DEF.pdf	VIK	VIK - Intern onderzoek-oriënterend	Bijzondere persoonsgegevens:gezondheidsgegevens				x	x	4	3	12	Hoog	Issue: Er is geen wettelijke uitzondering voor: Gezondheidsgegevens: (ii) of men medicijnen of andere middelen gebruikt die invloed kunnen hebben op het hoorgesprek met de VIK-onderzoeker (staat in standaard hoorverslag). Risico: Als deze gegevens worden gebruikt in het kader van oriënterende onderzoeken, gebeurt dit in strijd met de AVG. Juist bijzondere persoonsgegevens worden extra beschermd in de AVG gezien hun gevoelige aard, dus schending van deze regels heeft een nadelige impact op de persoonlijke levenssfeer van een betrokkene.	Deze vraag achterwege vragen in het hoorverslag. Er wordt al in meer algemene termen gevraagd of men in staat is aan het gesprek deel te nemen.	IB risico	1-1-2024

Privacy	20231026 GEB_AVG_Oriënterend Onderzoek_1.0_DEF.pdf	VIK	VIK - Intern onderzoek-oriënterend	Bijzondere persoonsgegevens:lidmaatschap vakbond				x		2	2	4	Midden	Issue: Lidmaatschap vakbond: indien een betrokkene zich laat bijstaan door een gemachtigde/jurist verbonden aan een vakbond en dit wordt vastgelegd, worden daarmee gegevens van betrokkene over lidmaatschap van een vakbond verwerkt. Lidmaatschap vakbond is een bijzonder persoonsgegeven en er kan geen beroep worden gedaan op een wettelijke uitzondering om dit bijzondere persoonsgegeven te mogen verwerken. Risico: Als deze gegevens worden verwerkt in het kader van oriënterende onderzoeken, gebeurt dit in strijd met de AVG.	Lidmaatschap vakbond wordt in Nederland in het algemeen niet als zeer kritisch ervaren. Daarom kan in dit risico worden voorzien door tijdens het hoorgesprek uitdrukkelijke toestemming te vragen voor vermelding hiervan en dit in het verslag op te nemen. Indien geen toestemming wordt gegeven, dan vermelding achterwege laten.	IB risico	1-1-2024
Privacy	20231026 GEB_AVG_Oriënterend Onderzoek_1.0_DEF.pdf	VIK	VIK - Intern onderzoek-oriënterend	Strafrechtelijke persoonsgegevens					x	2	5	10	Hoog	Issue: 5.1.2.i Risico: 5.1.2.i	5.1.2.i	IB risico	1-1-2024
Privacy	20231026 GEB_AVG_Oriënterend Onderzoek_1.0_DEF.pdf	VIK	VIK - Intern onderzoek-oriënterend	5.1.2.i				x	x	3	4	12	Hoog	Issue: 5.1.2.i Risico: 5.1.2.i	5.1.2.i 5.1.2.i	IB risico	1-1-2024
Privacy	20231026 GEB_AVG_Oriënterend Onderzoek_1.0_DEF.pdf	VIK	VIK - Intern onderzoek-oriënterend	Nationaliteit						3	4	12	Hoog	Issue: Van burgergetuigen wordt de nationaliteit genoteerd. Risico: Het risico bestaat dat op basis van nationaliteit discriminatie plaats vindt.	Stoppen met het vragen naar de nationaliteit. Dit kan door deze vraag uit het verslag burgergetuigen te schrappen.	IB risico	1-1-2024
Privacy	20231026 GEB_AVG_Oriënterend Onderzoek_1.0_DEF.pdf	VIK	VIK - Intern onderzoek-oriënterend	Opslag en verzending van gegevens			x	x	x	5	4	20	Zeer hoog	Issue: 5.1.2.i Risico: 5.1.2.i	5.1.2.i	IB risico	1-1-2024
Privacy	20231026 GEB_AVG_Oriënterend Onderzoek_1.0_DEF.pdf	VIK	VIK - Intern onderzoek-oriënterend	IB-risicoanalyse op Delta						3	3	9	Midden	Issue: Er is een IB-risico analyse op Delta opgeleverd. Bij de implementatie en beoordeling van de risico's is (nog) onvoldoende gekeken naar de privacy risico's. Risico: o.a. onrechtmatige gegevensverwerking	Kijk opnieuw naar de uitkomsten van de IB-analyse en beoordeel de risico's voor de privacy van de categorieën betrokkenen. Neem in deze beoordeling ook de geaccepteerde risico's mee.	IB risico	1-1-2024
Privacy	20231026 GEB_AVG_Oriënterend Onderzoek_1.0_DEF.pdf	VIK	VIK - Intern onderzoek-oriënterend	Doorgifte themaregister					x	3	5	15	Hoog	Issue: Persoonsgegevens uit een oriënterend onderzoek worden mogelijk verstrekt aan het themaregister ambtelijke omkoping. Risico: Betrokkene wordt ten onrechte gelabeld met een profiel van "gevoelig voor / betrokken bij ambtelijke omkoping".	Volg het advies van 5.1.2.e en 5.1.2.e vastgelegd in het memo d.d. 10 maart 2021 over verstrekking van gegevens aan het themaregister. Dit memo is als bijlage 4 aan de GEB gehecht.	IB risico	1-1-2024
Privacy	Definitief GEB Opbouwen informatiepositie CTER Jihadisme en Nationaal Extremisme versie 1.0.docx	CTER	Opbouwen informatiepositie CTER-Jihadisme-Nationaal Extremisme	Proportionaliteit					x	2	2	4	Midden	Issue: Er worden te veel gegevens verwerkt. Risico: datalek, stigmatisering en reputatieschade.	Stem met IB af over maatregelen in de systemen om dataminimalisatie te bereiken. Evalueer onderzoek uit verleden om te bepalen of alle gegevens noodzakelijk zijn.	IB risico	1-1-2024
Privacy	Definitief GEB Opbouwen informatiepositie CTER Jihadisme en Nationaal Extremisme versie 1.0.docx	CTER	Opbouwen informatiepositie CTER-Jihadisme-Nationaal Extremisme	Logging						3	2	6	Midden	Applicatiebeheer logt op persoonsniveau, niet centraal voor de hele politie ingericht. Verstrekkingen moeten worden gelogd. Voor VIK wordt gelogd.	Richt een logging procedure in welke is gericht op de verwerking en zorg voor betere monitoring op de logging.	IB risico	1-1-2024
Privacy	Definitief GEB Opbouwen informatiepositie CTER Jihadisme en Nationaal Extremisme versie 1.0.docx	CTER	Opbouwen informatiepositie CTER-Jihadisme-Nationaal Extremisme	Wetenschap					x	3	2	6	Midden	Issue: De verstrekking voor beleidsinformatie, wetenschappelijk onderzoek of statistiek kan ten onrechte leiden tot resultaten met persoonsgegevens. Risico: imago schade, herleiding tot persoon	Anonimiseer de gegevens voordat je toegang geeft aan onderzoekers.	IB risico	1-1-2024
Privacy	Definitief GEB Opbouwen informatiepositie CTER Jihadisme en Nationaal Extremisme versie 1.0.docx	CTER	Opbouwen informatiepositie CTER-Jihadisme-Nationaal Extremisme	5.1.2.i			x	x	x	5	4	20	Zeer hoog	Issue: 5.1.2.i	5.1.2.i	IB risico	1-1-2024
Privacy	Definitief GEB Opbouwen informatiepositie CTER Jihadisme en Nationaal Extremisme versie 1.0.docx	CTER	Opbouwen informatiepositie CTER-Jihadisme-Nationaal Extremisme	Verwerkingstermijnen					x	5	4	20	Zeer hoog	Issue: De verwerkingstermijnen mbt vernietigen worden niet nageleefd. Risico: o.a. onrechtmatige gegevensverwerking	Pas systemen en procedures aan om de verwerkingstermijnen van de Wpg correct na te leven.	IB risico	1-1-2024
Privacy	Definitief GEB Opbouwen informatiepositie CTER Jihadisme en Nationaal Extremisme versie 1.0.docx	CTER	Opbouwen informatiepositie CTER-Jihadisme-Nationaal Extremisme	5.1.2.i					x	2	4	8	Midden	Issue: 5.1.2.i Risico: 5.1.2.i	5.1.2.i 5.1.2.i	Werkproces gerelateerd	1-1-2024

Privacy	Definitief GEB Opbouwen informatiepositie CTER Jihadisme en Nationaal Extremisme versie 1.0.docx	CTER	Opbouwen informatiepositie CTER-Jihadisme-Nationaal Extremisme	[redacted]						3	4	12	Hoog	Issue: [redacted] Risico: [redacted]	[redacted]	IB risico	1-1-2024
Privacy	Definitief GEB Opbouwen informatiepositie CTER Jihadisme en Nationaal Extremisme versie 1.0.docx	CTER	Opbouwen informatiepositie CTER-Jihadisme-Nationaal Extremisme	Contractuele afspraken					x	4	4	16	Hoog	Issue: Er ontbreken afspraken met de leverancier of een andere externe partij over de verwerking van politiegegevens en de informatiebeveiliging. Risico: o.a. datalek	Maak passende afspraken met de leverancier betreffende de verwerking van politiegegevens die voldoen aan de privacywetgeving en informatiebeveiliging voor tijdens onderhoud.	IB risico	1-1-2024
Privacy	Definitief GEB Opbouwen informatiepositie CTER Jihadisme en Nationaal Extremisme versie 1.0.docx	CTER	Opbouwen informatiepositie CTER-Jihadisme-Nationaal Extremisme	Kennis					x	3	4	12	Hoog	Issue: De bevoegde functionarissen blijken onvoldoende op de hoogte van de privacy regels mbt verstrekkingen aan derde door gebruik van applicaties. – politie breed issue van training. Wel onderdeel van CTER opleiding. Risico: o.a. datalekken	Geef regelmatig op de verwerking gerichte privacytraining.	IB risico	1-1-2024
Privacy	Definitief GEB Opbouwen informatiepositie CTER Jihadisme en Nationaal Extremisme versie 1.0.docx	CTER	Opbouwen informatiepositie CTER-Jihadisme-Nationaal Extremisme	Verwerkingstermijnen					x	5	4	20	Zeer hoog	Issue: De verwerkingstermijnen mbt vernietigen worden niet nageleefd. Risico: o.a. onrechtmatige gegevensverwerking	Pas systemen en procedures aan om de verwerkingstermijnen van de Wpg correct na te leven.	IB risico	1-1-2024
Privacy	Definitief GEB Opbouwen informatiepositie CTER Jihadisme en Nationaal Extremisme versie 1.0.docx	CTER	Opbouwen informatiepositie CTER-Jihadisme-Nationaal Extremisme	[redacted]					x	2	4	8	Midden	Issue: [redacted] Risico: [redacted]	Afstemming met IB over maatregel en hierin kopiëren. [redacted]	Werkproces gerelateerd	1-1-2024
Privacy	Definitief GEB Opbouwen informatiepositie CTER Jihadisme en Nationaal Extremisme versie 1.0.docx	CTER	Opbouwen informatiepositie CTER-Jihadisme-Nationaal Extremisme	Kennis					x	3	4	12	Hoog	Issue: De bevoegde functionarissen blijken onvoldoende op de hoogte van de privacy regels mbt verstrekkingen aan derde door gebruik van applicaties. – politie breed issue van training. Wel onderdeel van CTER opleiding. Risico: o.a. datalekken	Geef regelmatig op de verwerking gerichte privacytraining.	IB risico	1-1-2024
Privacy	Definitief GEB Opbouwen informatiepositie CTER Jihadisme en Nationaal Extremisme versie 1.0.docx	CTER	Opbouwen informatiepositie CTER-Jihadisme-Nationaal Extremisme	Proportionaliteit					x	2	2	4	Midden	Issue: Er worden te veel gegevens verwerkt. Risico: datalek, stigmatisering en reputatieschade.	Stem met IB af over maatregelen in de systemen om dataminimalisatie te bereiken. Evalueer onderzoek uit verleden om te bepalen of alle gegevens noodzakelijk zijn.	IB risico	1-1-2024
Privacy	Definitief GEB Opbouwen informatiepositie CTER Jihadisme en Nationaal Extremisme versie 1.0.docx	CTER	Opbouwen informatiepositie CTER-Jihadisme-Nationaal Extremisme	Logging						3	2	6	Midden	Applicatiebeheer logt op persoonsniveau, niet centraal voor de hele politie ingericht. Verstrekkingen moeten worden gelogd. Voor VIK wordt gelogd.	Richt een logging procedure in welke is gericht op de verwerking en zorg voor betere monitoring op de logging.	IB risico	1-1-2024
Privacy	Definitief GEB Opbouwen informatiepositie CTER Jihadisme en Nationaal Extremisme versie 1.0.docx	CTER	Opbouwen informatiepositie CTER-Jihadisme-Nationaal Extremisme	[redacted]						3	4	12	Hoog	Issue: [redacted] Risico: [redacted]	[redacted]	IB risico	1-1-2024
Privacy	Definitief GEB Opbouwen informatiepositie CTER Jihadisme en Nationaal Extremisme versie 1.0.docx	CTER	Opbouwen informatiepositie CTER-Jihadisme-Nationaal Extremisme	[redacted]			x	x	x	5	4	20	Zeer hoog	Issue: [redacted]	[redacted]	IB risico	1-1-2024
Privacy	Definitief GEB Opbouwen informatiepositie CTER Jihadisme en Nationaal Extremisme versie 1.0.docx	CTER	Opbouwen informatiepositie CTER-Jihadisme-Nationaal Extremisme	Contractuele afspraken					x	4	4	16	Hoog	Issue: Er ontbreken afspraken met de leverancier of een andere externe partij over de verwerking van politiegegevens en de informatiebeveiliging. Risico: o.a. datalek	Maak passende afspraken met de leverancier betreffende de verwerking van politiegegevens die voldoen aan de privacywetgeving en informatiebeveiliging voor tijdens onderhoud.	IB risico	1-1-2024
Privacy	Definitief GEB Opbouwen informatiepositie CTER Jihadisme en Nationaal Extremisme versie 1.0.docx	CTER	Opbouwen informatiepositie CTER-Jihadisme-Nationaal Extremisme	Wetenschap					x	3	2	6	Midden	Issue: De verstrekking voor beleidsinformatie, wetenschappelijk onderzoek of statistiek kan ten onrechte leiden tot resultaten met persoonsgegevens. Risico: imago schade, herleiding tot persoon	Anonimiseer de gegevens voordat je toegang geeft aan onderzoekers.	IB risico	1-1-2024
Privacy	Definitief GEB Opbouwen informatiepositie CTER Jihadisme en Nationaal Extremisme versie 1.0.docx	CTER	Opbouwen informatiepositie CTER-Jihadisme-Nationaal Extremisme	Verwerkingstermijnen					x	5	4	20	Zeer hoog	Issue: De verwerkingstermijnen m.b.t. vernietigen worden niet nageleefd. Risico: o.a. onrechtmatige gegevensverwerking	Pas systemen en procedures aan om de verwerkingstermijnen van de Wpg correct na te leven.	IB risico	1-1-2024
Privacy	Definitief GEB Opbouwen informatiepositie CTER Jihadisme en Nationaal Extremisme versie 1.0.docx	CTER	Opbouwen informatiepositie CTER-Jihadisme-Nationaal Extremisme	[redacted]					x	2	4	8	Midden	Issue: [redacted] Risico: [redacted]	[redacted]	Werkproces gerelateerd	1-1-2024
Privacy	Definitief GEB Opbouwen informatiepositie CTER Jihadisme en Nationaal Extremisme versie 1.0.docx	CTER	Opbouwen informatiepositie CTER-Jihadisme-Nationaal Extremisme	Kennis					x	3	4	12	Hoog	Issue: De bevoegde functionarissen blijken onvoldoende op de hoogte van de privacy regels m.b.t. verstrekkingen aan derde door gebruik van applicaties. – politie breed issue van training. Wel onderdeel van CTER opleiding. Risico: o.a. datalekken	Geef regelmatig op de verwerking gerichte privacy training	IB risico	1-1-2024

Privacy	Definitief GEB Opbouwen informatiepositie CTER Jihadisme en Nationaal Extremisme versie 1.0.docx	CTER	Opbouwen informatiepositie CTER-Jihadisme-Nationaal Extremisme	Proportionaliteit					x	2	2	4	Midden	Issue: Er worden te veel gegevens verwerkt. Risico: datalek, stigmatisering en reputatieschade.	Stem met IB af over maatregelen in de systemen om dataminimalisatie te bereiken. Evalueer onderzoek uit verleden om te bepalen of alle gegevens noodzakelijk zijn.	IB risico	1-1-2024
Privacy	Definitief GEB Opbouwen informatiepositie CTER Jihadisme en Nationaal Extremisme versie 1.0.docx	CTER	Opbouwen informatiepositie CTER-Jihadisme-Nationaal Extremisme	Logging						2	3	6	Midden	Applicatiebeheer logt op persoonsniveau, niet centraal voor de hele politie ingericht. Verstrekkingen moeten worden gelogd. Voor VIK wordt gelogd.	Richt een logging procedure in welke is gericht op de verwerking en zorg voor betere monitoring op de logging.	IB risico	1-1-2024
Privacy	Definitief GEB Opbouwen informatiepositie CTER Jihadisme en Nationaal Extremisme versie 1.0.docx	CTER	Opbouwen informatiepositie CTER-Jihadisme-Nationaal Extremisme	5.1.2.i						3	4	12	Hoog	Issue: 5.1.2.i Risico: 5.1.2.i	5.1.2.i	IB risico	1-1-2024
Privacy	Definitief GEB Opbouwen informatiepositie CTER Jihadisme en Nationaal Extremisme versie 1.0.docx	CTER	Opbouwen informatiepositie CTER-Jihadisme-Nationaal Extremisme	5.1.2.i			x	x	x	5	4	20	Zeer hoog	Issue: 5.1.2.i	5.1.2.i	IB risico	1-1-2024
Privacy	Definitief GEB Opbouwen informatiepositie CTER Jihadisme en Nationaal Extremisme versie 1.0.docx	CTER	Opbouwen informatiepositie CTER-Jihadisme-Nationaal Extremisme	Contractuele afspraken					x	4	4	16	Hoog	Issue: Er ontbreken afspraken met de leverancier of een andere externe partij over de verwerking van politiegegevens en de informatiebeveiliging. Risico: o.a. datalek	Maak passende afspraken met de leverancier betreffende de verwerking van politiegegevens die voldoen aan de privacywetgeving en informatiebeveiliging voor tijdens onderhoud.	IB risico	1-1-2024
Privacy	Definitief GEB Opbouwen informatiepositie CTER Jihadisme en Nationaal Extremisme versie 1.0.docx	CTER	Opbouwen informatiepositie CTER-Jihadisme-Nationaal Extremisme	Wetenschap					x	3	2	6	Midden	Issue: De verstrekking voor beleidsinformatie, wetenschappelijk onderzoek of statistiek kan ten onrechte leiden tot resultaten met persoonsgegevens. Risico: imago schade, herleiding tot persoon	Anonimiseer de gegevens voordat je toegang geeft aan onderzoekers.	IB risico	1-1-2024
Privacy	GEB Screening versie 1.0.pdf	VIK	VIK-Screening	5.1.2.i			x		x	5	4	20	Zeer hoog	Issue: 5.1.2.i Risico: 5.1.2.i	5.1.2.i	IB risico	1-1-2024
Privacy	GEB Screening versie 1.0.pdf	VIK	VIK-Screening	Beveiligd delen van informatie					x	5	4	20	Zeer hoog	Issue: 5.1.2.i Risico: 5.1.2.i	Richt het screeningsproces zo in dat persoonsgegevens na de aanvraag alleen door VIK-screening worden verwerkt.	IB risico	1-1-2024
Privacy	GEB Screening versie 1.0.pdf	VIK	VIK-Screening	Apart register in de zin van Artikel 10 Besluit Screening						3	3	9	Midden	Issue: Er is een IB-risico analyse op Delta opgeleverd. Bij de implementatie en beoordeling van de risico's is (nog) onvoldoende gekeken naar de privacy risico's. Risico: o.a. onrechtmatige gegevensverwerking	Kijk opnieuw naar de uitkomsten van de IB-analyse en beoordeel de risico's voor de privacy van de categorieën betrokkenen. Neem in deze beoordeling ook de geaccepteerde risico's mee.	IB risico	1-1-2024
Privacy	GEB Screening versie 1.0.pdf	VIK	VIK-Screening	Er is te weinig privacy ondersteuning voor het VIK				x		3	3	9	Midden	Issue: Functionarissen weten niet welke privacyfunctionaris of privacy adviseur de VIKs adviseert over privacy gerelateerde vraagstukken. Risico: Mogelijke onjuiste gegevensverwerking doordat advies mogelijk niet of beperkt ingewonnen kan worden.	Wijs een privacyfunctionaris/adviseur aan die specifiek en vakinhoudelijk op privacy gerelateerde vraagstukken kan ondersteunen binnen het screeningsproces.	IB risico	1-1-2024
Privacy	GEB Screening versie 1.0.pdf	VIK	VIK-Screening	Autorisatie			x		x	3	5	15	Hoog	Issue: 5.1.2.i Risico: 5.1.2.i	5.1.2.i	IB risico	1-1-2024
Privacy	GEB Screening versie 1.0.pdf	VIK	VIK-Screening	Autorisatie					x	3	5	15	Hoog	Issue: Autorisaties worden niet (periodiek) gecontroleerd 5.1.2.i	Controleer en beheer periodiek of de uitgegeven autorisaties nog actueel zijn en noodzakelijk zijn voor de uitoefening van de functie.	IB risico	1-1-2024
Privacy	GEB Screening versie 1.0.pdf	VIK	VIK-Screening	Bewaartermijnen				x		4	5	20	Zeer hoog	Issue: De bewaartermijn wordt niet nageleefd. Het is niet mogelijk in Delta om geautomatiseerd gegevens te verwijderen. Ook de naleving van de bewaartermijnen op andere platforms zoals mail en schijven is niet geborgd. Risico: o.a. onrechtmatige gegevensverwerking omdat de verwerking te lang plaatsvindt.	Pas systemen en procedures aan om de bewaartermijnen na te leven.	IB risico	1-1-2024
Privacy	GEB Screening versie 1.0.pdf	VIK	VIK-Screening	De rechten van betrokkenen kunnen niet goed worden uitgevoerd				x	x	4	2	8	Midden	Issue: De folder 'Zo screent de politie' over het screeningsproces is verouderd. Risico: Mogelijk onjuiste of onrechtmatige gegevensverwerking omdat de betrokkenen niet goed en niet volledig geïnformeerd zijn en hun rechten dus niet goed kunnen uitvoeren.	Pas de folder 'Zo screent de politie' aan zodat de verwerking voor de betrokkene inzichtelijk is en voldaan wordt aan de informatieverplichtingen uit de AVG.	IB risico	1-1-2024
Privacy	GEB Screening versie 1.0.pdf	VIK	VIK-Screening	Kennis			x		x	2	4	8	Midden	Issue: De functionarissen zijn mogelijk onvoldoende op de hoogte van de privacyregels. Voornamelijk als het gaat om bewaren, opslaan en het opnemen van gegevens. Risico: o.a. onrechtmatige gegevensverwerking en datalekken	Geef regelmatig (zoveel mogelijk op de verwerking gerichte) privacy training. Denk hierbij aan een certificering voor toegang.	IB risico	1-1-2024
Privacy	GEB Screening versie 1.0.pdf	VIK	VIK-Screening	5.1.2.i				x	x	5	4	20	Zeer hoog	Issue: 5.1.2.i Risico: 5.1.2.i	5.1.2.i	IB risico	1-1-2024
Privacy	GEB Screening versie 1.0.pdf	VIK	VIK-Screening	Proportionaliteit				x	x	4	5	20	Zeer hoog	Issue: Er worden te veel persoonsgegevens verwerkt. Risico: datalek en reputatieschade. Doordat er in het screeningsproces te veel persoonsgegevens worden verwerkt ontstaat er een te ruim beeld over de betrokkene en loopt de politieorganisatie risico op mogelijke sancties.	Scherp de verwerking aan op het wettelijke kader, noodzaak, het doel en geef richtlijnen hoe de doelen efficiënt kunnen worden bereikt. Kijk hierover in ieder geval naar het OPG-formulier en de aantekeningenlijst.	IB risico	1-1-2024

Privacy	GEB Screening versie 1.0.pdf	VIK	VIK-Screening	Bijzondere persoonsgegevens					x	4	4	16	Hoog	Issue: 5.1.2.i Risico: 5.1.2.i	5.1.2.i	B risico	1-1-2024
Privacy	GEB Screening versie 1.0.pdf	VIK	VIK-Screening	Autorisatie			x		x	3	5	15	Hoog	Issue: Er is geen autorisatiebeleid of autorisatiematrix beschikbaar voor deze verwerking. Risico: o.a. datalekken en onrechtmatig gegevensgebruik. Er kunnen (mogelijk) meer mensen bij gegevens dan voor hun taak noodzakelijk is.	Stel autorisatiematrixen op per gebruikt systeem door VIK-screening.	IB risico	1-1-2024
Privacy	GEB Screening versie 1.0.pdf	VIK	VIK-Screening	Autorisatie					x	3	5	15	Hoog	Issue: Autorisaties worden niet (periodiek) gecontroleerd en beheerd. Risico: o.a. datalekken en onrechtmatig gegevensgebruik. Er kunnen (mogelijk) meer mensen bij gegevens dan voor hun taak noodzakelijk is.	Controleer en beheer periodiek of de uitgegeven autorisaties nog actueel zijn en noodzakelijk zijn voor de uitoefening van de functie.	IB risico	1-1-2024
Privacy	GEB Screening versie 1.0.pdf	VIK	VIK-Screening	Bewaartermijnen				x		4	5	20	Zeer hoog	Issue: De bewaartermijn wordt niet nageleefd. Het is niet mogelijk in Delta om geautomatiseerd gegevens te verwijderen. Ook de naleving van de bewaartermijnen op andere platforms zoals mail en schijven is niet geborgd. Risico: o.a. onrechtmatige gegevensverwerking omdat de verwerking te lang plaatsvindt.	Pas systemen en procedures aan om de bewaartermijnen na te leven.	IB risico	1-1-2024
Privacy	GEB Screening versie 1.0.pdf	VIK	VIK-Screening	De rechten van betrokkenen kunnen niet goed worden uitgevoerd				x	x	4	2	8	Midden	Issue: De folder 'Zo screent de politie' over het screeningsproces is verouderd. Risico: Mogelijk onjuiste of onrechtmatige gegevensverwerking omdat de betrokkenen niet goed en niet volledig geïnformeerd zijn en hun rechten dus niet goed kunnen uitvoeren.	Pas de folder 'Zo screent de politie' aan zodat de verwerking voor de betrokkene inzichtelijk is en voldaan wordt aan de informatieverplichtingen uit de AVG.	IB risico	1-1-2024
Privacy	GEB Screening versie 1.0.pdf	VIK	VIK-Screening	Er is te weinig privacy ondersteuning voor het VIK				x		3	3	9	Midden	Issue: Functionarissen weten niet welke privacyfunctionaris of privacy adviseur de VIKs adviseert over privacy gerelateerde vraagstukken. Risico: Mogelijke onjuiste gegevensverwerking doordat advies mogelijk niet of beperkt ingewonnen kan worden.	Wijs een privacyfunctionaris/adviseur aan die specifiek en vakinhoudelijk op privacy gerelateerde vraagstukken kan ondersteunen binnen het screeningsproces.	IB risico	1-1-2024
Privacy	GEB Screening versie 1.0.pdf	VIK	VIK-Screening	Kennis			x		x	2	4	8	Midden	Issue: De functionarissen zijn mogelijk onvoldoende op de hoogte van de privacyregels. Voornamelijk als het gaat om bewaren, opslaan en het opnemen van gegevens. Risico: o.a. onrechtmatige gegevensverwerking en datalekken	Geef regelmatig (zoveel mogelijk op de verwerking gerichte) privacy training. Denk hierbij aan een certificering voor toegang.	IB risico	1-1-2024
Privacy	GEB Screening versie 1.0.pdf	VIK	VIK-Screening	5.1.2.i			x		x	5	4	20	Zeer hoog	Issue: 5.1.2.i Risico: 5.1.2.i	5.1.2.i	IB risico	1-1-2024
Privacy	GEB Screening versie 1.0.pdf	VIK	VIK-Screening	Proportionaliteit				x	x	4	5	20	Zeer hoog	Issue: Er worden te veel persoonsgegevens verwerkt. Risico: datalek en reputatieschade. Doordat er in het screeningsproces te veel persoonsgegevens worden verwerkt ontstaat er een te ruim beeld over de betrokkene en loopt de politieorganisatie risico op mogelijke sancties.	Scherp de verwerking aan op het wettelijke kader, noodzaak, het doel en geef richtlijnen hoe de doelen efficiënt kunnen worden bereikt. Kijk hierover in ieder geval naar het OPG-formulier en de aantekeningenlijst.	IB risico	1-1-2024
Privacy	GEB Screening versie 1.0.pdf	VIK	VIK-Screening	Bijzondere persoonsgegevens					x	4	4	16	Hoog	Issue: 5.1.2.i Risico: 5.1.2.i	5.1.2.i	IB risico	1-1-2024
Privacy	GEB Screening versie 1.0.pdf	VIK	VIK-Screening	Beveiligd delen van informatie				x	x	5	4	20	Zeer hoog	Issue: 5.1.2.i Risico: 5.1.2.i	Richt een systeem in zodat VIK-medewerkers een dossier kunnen opbouwen in een veilige omgeving.	IB risico	1-1-2024
Privacy	GEB Screening versie 1.0.pdf	VIK	VIK-Screening	Beveiligd delen van informatie					x	5	4	20	Zeer hoog	Issue: 5.1.2.i Risico: 5.1.2.i	Richt het screeningsproces zo in dat persoonsgegevens na de aanvraag alleen door VIK-screening worden verwerkt.	IB risico	1-1-2024
Privacy	GEB Screening versie 1.0.pdf	VIK	VIK-Screening	Apart register in de zin van Artikel 10 Besluit Screening						3	3	9	Midden	Issue: Er is een IB-risico analyse op Delta opgeleverd. Bij de implementatie en beoordeling van de risico's is (nog) onvoldoende gekeken naar de privacy risico's. Risico: o.a. onrechtmatige gegevensverwerking	Kijk opnieuw naar de uitkomsten van de IB-analyse en beoordeel de risico's voor de privacy van de categorieën betrokkenen. Neem in deze beoordeling ook de geaccepteerde risico's mee.	IB risico	1-1-2024
Privacy	GEB UAV versie 1.0.DOCX	Landelijke eenheid	UAV Drones	5.1.2.i						3	5	15	Hoog	5.1.2.i	5.1.2.i	IB risico	1-1-2024
Privacy	GEB UAV versie 1.0.DOCX	Landelijke eenheid	UAV Drones	5.1.2.i			x			3	5	15	Hoog	5.1.2.i	5.1.2.i	IB risico	1-1-2024
Privacy	GEB UAV versie 1.0.DOCX	Landelijke eenheid	UAV Drones	5.1.2.i				x		3	5	15	Hoog	5.1.2.i	5.1.2.i	Werkproces gerelateerd	1-1-2024
Privacy	GEB UAV versie 1.0.DOCX	Landelijke eenheid	UAV Drones	5.1.2.i					x	5	2	10	Hoog	5.1.2.i	5.1.2.i	IB risico	1-1-2024

Privacy	GEB UAV versie 1.0.DOCX	Landelijke eenheid	UAV Drones	5.1.2.i					x	3	5	15	Hoog	5.1.2.i	5.1.2.i	IB risico	1-1-2024
Privacy	GEB Verhoren, 18-07-2023.pdf	Generieke Opsporing	Verhoren	Werkproces						1	2	2	Laag	Issue: De verwerking heeft een verouderd werkproces in de bedrijfsarchitectuur. Risico: o.a. de verwerking is niet transparant	Zorg dat de werkprocessen geactualiseerd worden, centraal vastgesteld en vastgelegd zijn en beschikbaar zijn gesteld aan de mensen die hiermee werken.	Werkproces gerelateerd	1-1-2024
Privacy	GEB Verhoren, 18-07-2023.pdf	Generieke Opsporing	Verhoren	Autorisatie					x	3	3	9	Midden	Issue: 5.1.2.i Risico: 5.1.2.i	5.1.2.i	IB risico	1-1-2024
Privacy	GEB Verhoren, 18-07-2023.pdf	Generieke Opsporing	Verhoren	Verwerkingstermijnen						4	3	12	Hoog	Issue: De verwerkingstermijnen worden niet nageleefd. Risico: onrechtmatige gegevensverwerking.	Implementeren van de wettelijke bewaartermijnen in samenwerking met een privacy adviseur/ jurist. Indien er niet aan alle wettelijke vereisten kan worden voldaan, het risico laten accepteren op niveau portefeuillehouder.	IB risico	1-1-2024
Privacy	GEB Verhoren, 18-07-2023.pdf	Generieke Opsporing	Verhoren	Bewaren en vernietigen					x	3	3	9	Midden	Issue: Geen duidelijk onderscheid tussen bewaren en vernietigen van gegevens. Risico: onrechtmatige gegevensverwerking, geen gegevens die vernietigd worden.	Zorg voor onderscheid tussen bewaren en vernietigen, bijvoorbeeld via een e-learning, maar ook in de onderliggende systemen dient dit ingeregeld te zijn. Zorg voor een Poortwachter.	IB risico	1-1-2024
Privacy	GEB Verhoren, 18-07-2023.pdf	Generieke Opsporing	Verhoren	Kennis en bewustwording				x		x	2	4	8	Midden	Issue: De functionarissen zijn mogelijk onvoldoende op de hoogte van de privacywetgeving. Voornamelijk als het gaat om bewaren, opslaan, delen/verstrekken en het opnemen van gegevens. Risico: o.a. datalekken Risico: Kans op afwijkend gedrag ten opzichte van de IB-standaarden.	Geef regelmatig (zoveel mogelijk op de verwerking gerichte) privacy training. Denk hierbij aan een certificering voor toegang.	IB risico	1-1-2024
Privacy	GEB Verhoren, 18-07-2023.pdf	Generieke Opsporing	Verhoren	Bewaren					x	3	3	9	Midden	Issue: Er wordt niet correct bewaard. Risico: imagoschade, toezichthouderboete, datalek, onrechtmatig gegevensgebruik	5.1.2.i	IB risico	1-1-2024
Privacy	GEB Verhoren, 18-07-2023.pdf	Generieke Opsporing	Verhoren	Gegevensbescherming		NCSC top-8 item	x		x	2	4	8	Midden	Issue: 5.1.2.i Risico: 5.1.2.i	5.1.2.i	IB risico	1-1-2024
Privacy	GEB Verhoren, 18-07-2023.pdf	Generieke Opsporing	Verhoren	Verstrekken gegevens				x	x	2	2	4	Midden	Issue: 5.1.2.i Risico: 5.1.2.i	Gebruik langere encryptie-wachtwoorden bij verstrekkingen: Bij het gebruik van alfanumerieke wachtwoorden van 20 karakters, is het aantal mogelijkheden ongeveer 10^35. Door het gebruik van wachtwoorden van deze lengte worden bruteforce-aanvallen praktisch onhaalbaar.	IB risico	1-1-2024
Privacy	GEB Verhoren, 18-07-2023.pdf	Generieke Opsporing	Verhoren	Niet bovenmatig					x	2	1	2	Laag	Issue: Sommige persoonsgegevens die worden verwerkt tijdens het verhoor liggen met name in de sfeer van hetgeen wordt verklaard tijdens een verhoor. Hiervan is tijdens het verhoor niet vast te stellen of dit bovenmatig is.	Geef werkinstructies/ verhoortrainingen om overbodige verwerkingen te voorkomen.	Werkproces gerelateerd	1-1-2024
Privacy	GEB Verhoren, 18-07-2023.pdf	Generieke Opsporing	Verhoren	Eenmalige vastlegging				x		3	3	9	Midden	Issue: Gegevens AVR worden niet geverifieerd in de basisregistratie. Risico: Onjuiste gegevensverwerking	Zorg dat gegevens van een kernobject worden geverifieerd in de betreffende basisregistratie.	IB risico	1-1-2024
Privacy	GEB Verhoren, 18-07-2023.pdf	Generieke Opsporing	Verhoren	Onjuistheden terug melden				x		2	3	6	Midden	Issue: AVR ondersteunt geen terugmeldvoorziening Risico: Onjuiste gegevensverwerking	Zorg dat onjuistheden aan de bronhouder kunnen worden teruggemeld. Volgens de 0-meting van AVR is dit technisch wel mogelijk is, maar wordt het niet toegepast.	IB risico	1-1-2024
Privacy	GEB Verhoren, 18-07-2023.pdf	Generieke Opsporing	Verhoren	Duurzame toegankelijkheid			x		x	3	4	12	Hoog	Issue: 5.1.2.i Risico: 5.1.2.i	5.1.2.i	IB risico	1-1-2024
Privacy	GEB Verhoren, 18-07-2023.pdf	Generieke Opsporing	Verhoren	Werkproces						1	2	2	Laag	Issue: De verwerking heeft een verouderd werkproces in de bedrijfsarchitectuur. Risico: o.a. de verwerking is niet transparant	Zorg dat de werkprocessen geactualiseerd worden, centraal vastgesteld en vastgelegd zijn en beschikbaar zijn gesteld aan de mensen die hiermee werken.	Werkproces gerelateerd	1-1-2024
Privacy	GEB Verhoren, 18-07-2023.pdf	Generieke Opsporing	Verhoren	Autorisatie					x	3	3	9	Midden	Issue: Er is geen duidelijk aangegeven functionaris die het autorisatiebeleid of de autorisatiematrix voor deze verwerking beheert. Risico: o.a. datalekken en onrechtmatig gegevensgebruik.	Benoem, of maak duidelijk, wie de functionaris is die de autorisatiematrix beheert en zorg voor een e-learning om de kennis op peil te brengen/houden.	IB risico	1-1-2024
Privacy	GEB Verhoren, 18-07-2023.pdf	Generieke Opsporing	Verhoren	Verwerkingstermijnen						4	3	12	Hoog	Issue: De verwerkingstermijnen worden niet nageleefd. Risico: onrechtmatige gegevensverwerking.	Implementeren van de wettelijke bewaartermijnen in samenwerking met een privacy adviseur/ jurist. Indien er niet aan alle wettelijke vereisten kan worden voldaan, het risico laten accepteren op niveau portefeuillehouder.	IB risico	1-1-2024
Privacy	GEB Verhoren, 18-07-2023.pdf	Generieke Opsporing	Verhoren	Bewaren en vernietigen					x	3	3	9	Midden	Issue: Geen duidelijk onderscheid tussen bewaren en vernietigen van gegevens. Risico: onrechtmatige gegevensverwerking, geen gegevens die vernietigd worden.	Zorg voor onderscheid tussen bewaren en vernietigen, bijvoorbeeld via een e-learning, maar ook in de onderliggende systemen dient dit ingeregeld te zijn. Zorg voor een Poortwachter.	IB risico	1-1-2024
Privacy	GEB Verhoren, 18-07-2023.pdf	Generieke Opsporing	Verhoren	Kennis en bewustwording				x		x	2	4	8	Midden	Issue: De functionarissen zijn mogelijk onvoldoende op de hoogte van de privacywetgeving. Voornamelijk als het gaat om bewaren, opslaan, delen/verstrekken en het opnemen van gegevens. Risico: o.a. datalekken Risico: Kans op afwijkend gedrag ten opzichte van de IB-standaarden.	Geef regelmatig (zoveel mogelijk op de verwerking gerichte) privacy training. Denk hierbij aan een certificering voor toegang.	IB risico	1-1-2024
Privacy	GEB Verhoren, 18-07-2023.pdf	Generieke Opsporing	Verhoren	Bewaren					x	3	3	9	Midden	Issue: Er wordt niet correct bewaard. Risico: imagoschade, toezichthouderboete, datalek, onrechtmatig gegevensgebruik	5.1.2.i	IB risico	1-1-2024
Privacy	GEB Verhoren, 18-07-2023.pdf	Generieke Opsporing	Verhoren	Gegevensbescherming		NCSC top-8 item	x		x	2	4	8	Midden	Issue 5.1.2.i Risico: datalek	5.1.2.i	IB risico	1-1-2024

Privacy	GEB Verhoren, 18-07-2023.pdf	Generieke Opsporing	Verhoren	5.1.2.i				x	x	2	2	4	Midden	Issue: 5.1.2.i Risico: 5.1.2.i	Gebruik langere encryptie-wachtwoorden bij verstrekkingen: Bij het gebruik van alfanumerieke wachtwoorden van 20 karakters, is het aantal mogelijkheden ongeveer 10^35. Door het gebruik van wachtwoorden van deze lengte worden bruteforce-aanvallen praktisch onhaalbaar.	IB risico	1-1-2024
Privacy	GEB Verhoren, 18-07-2023.pdf	Generieke Opsporing	Verhoren	Niet bovenmatig					x	2	1	2	Laag	Issue: Sommige persoonsgegevens die worden verwerkt tijdens het verhoor liggen met name in de sfeer van hetgeen wordt verklaard tijdens een verhoor. Hiervan is tijdens het verhoor niet vast te stellen of dit bovenmatig is.	Geef werkinstructies/ verhoortrainingen om overbodige verwerkingen te voorkomen.	Werkproces gerelateerd	1-1-2024
Privacy	GEB Verhoren, 18-07-2023.pdf	Generieke Opsporing	Verhoren	Eenmalige vastlegging				x		3	3	9	Midden	Issue: Gegevens AVR worden niet geverifieerd in de basisregistratie. Risico: Onjuiste gegevensverwerking	Zorg dat gegevens van een kernobject worden geverifieerd in de betreffende basisregistratie.	IB risico	1-1-2024
Privacy	GEB Verhoren, 18-07-2023.pdf	Generieke Opsporing	Verhoren	Onjuistheden terug melden				x		2	3	6	Midden	Issue: AVR ondersteunt geen terugmeldvoorziening Risico: Onjuiste gegevensverwerking	Zorg dat onjuistheden aan de bronhouder kunnen worden teruggemeld. Volgens de 0-meting van AVR is dit technisch wel mogelijk is, maar wordt het niet toegepast.	IB risico	1-1-2024
Privacy	GEB Verhoren, 18-07-2023.pdf	Generieke Opsporing	Verhoren	Duurzame toegankelijkheid			x		x	3	4	12	Hoog	Issue: 5.1.2.i Risico: 5.1.2.i	Zorg voor e-learning AVR voor het opslaan van verhoren danwel voor een duurzaam toegankelijk systeem.	IB risico	1-1-2024
Privacy	GEB Verhoren, 18-07-2023.pdf	Generieke Opsporing	Verhoren	Autorisaties					x	4	5	20	Zeer hoog	Issue: 5.1.2.i Risico: 5.1.2.i	5.1.2.i Zorg voor reguliere controle van de autorisaties volgens het beleid en de autorisatiematrixen.	Werkproces gerelateerd	1-1-2024
Privacy	GEB Verhoren, 18-07-2023.pdf	Generieke Opsporing	Verhoren	Autorisaties					x	4	5	20	Zeer hoog	Issue: 5.1.2.i Risico: 5.1.2.i	5.1.2.i	IB risico	1-1-2024
Privacy	GEB Verhoren, 18-07-2023.pdf	Generieke Opsporing	Verhoren	Autorisaties					x	3	5	15	Hoog	Issue: 5.1.2.i Risico: 5.1.2.i	Geef hierover trainingen en controleer het gebruik van autorisaties.	IB risico	1-1-2024
Privacy	GEB_AVG_Disciplinair Onderzoek_versie 1.0.pdf	VIK	VIK-Intern onderzoek-disciplinair	Autorisaties					x	4	5	20	Zeer hoog	Issue: 5.1.2.i Risico: 5.1.2.i	5.1.2.i Zorg voor reguliere controle van de autorisaties volgens het beleid en de autorisatiematrixen.	Werkproces gerelateerd	1-1-2024
Privacy	GEB_AVG_Disciplinair Onderzoek_versie 1.0.pdf	VIK	VIK-Intern onderzoek-disciplinair	Autorisaties					x	4	5	20	Zeer hoog	Issue: 5.1.2.i Risico: 5.1.2.i datalekken, boetes voor de organisatie.	5.1.2.i	IB risico	1-1-2024
Privacy	GEB_AVG_Disciplinair Onderzoek_versie 1.0.pdf	VIK	VIK-Intern onderzoek-disciplinair	Autorisaties					x	3	5	15	Hoog	Issue: 5.1.2.i Risico: 5.1.2.i	Geef hierover trainingen en controleer het gebruik van autorisaties.	IB risico	1-1-2024
Privacy	GEB_AVG_Disciplinair Onderzoek_versie 1.0.pdf	VIK	VIK-Intern onderzoek-disciplinair	5.1.2.i				x	x	2	5	10	Hoog	Issue: 5.1.2.i Risico: 5.1.2.i	5.1.2.i	IB risico	1-1-2024
Privacy	GEB_AVG_Disciplinair Onderzoek_versie 1.0.pdf	VIK	VIK-Intern onderzoek-disciplinair	Proportionaliteit en subsidiariteit					x	3	4	12	Hoog	Issue: 5.1.2.i Risico: Er worden mogelijk meer persoonsgegevens verwerkt dan noodzakelijk; 5.1.2.i	5.1.2.i	IB risico	1-1-2024
Privacy	GEB_AVG_Disciplinair Onderzoek_versie 1.0.pdf	VIK	VIK-Intern onderzoek-disciplinair	Bijzondere persoonsgegevens:gezondheidsgegevens			x		x	4	3	12	Hoog	Issue: Er is geen wettelijke uitzondering voor: Gezondheidsgegevens: (ii) of men medicijnen of andere middelen gebruikt die invloed kunnen hebben op het hoorgesprek met de VIK-onderzoeker (staat in standaard hoorverslag). Risico: Als deze gegevens worden gebruikt in het kader van disciplinaire onderzoeken, gebeurt dit in strijd met de AVG. Juist bijzondere persoonsgegevens worden extra beschermd in de AVG gezien hun gevoelige aard, dus schending van deze regels heeft een nadelige impact op de persoonlijke levenssfeer van een betrokkene.	Deze vraag achterwege vragen in het hoorverslag. Er wordt al in meer algemene termen gevraagd of men in staat is aan het gesprek deel te nemen.	IB risico	1-1-2024
Privacy	GEB_AVG_Disciplinair Onderzoek_versie 1.0.pdf	VIK	VIK-Intern onderzoek-disciplinair	Bijzondere persoonsgegevens:lidmaatschap vakbond				x		2	2	4	Midden	Issue: Lidmaatschap vakbond: indien een betrokkene zich laat bijstaan door een gemachtigde/jurist verbonden aan een vakbond en dit wordt vastgelegd, worden daarmee gegevens van betrokkene over lidmaatschap van een vakbond verwerkt. Lidmaatschap vakbond is een bijzonder persoonsgegeven en er kan geen beroep worden gedaan op een wettelijke uitzondering om dit bijzondere persoonsgegeven te mogen verwerken. Risico: Als deze gegevens worden verwerkt in het kader van disciplinaire onderzoeken, gebeurt dit in strijd met de AVG.	Lidmaatschap vakbond wordt in Nederland in het algemeen niet als zeer kritisch ervaren. Daarom kan in dit risico worden voorzien door tijdens het hoorgesprek uitdrukkelijke toestemming te vragen voor vermelding hiervan en dit in het verslag op te nemen. Indien geen toestemming wordt gegeven, dan vermelding achterwege laten.	IB risico	1-1-2024
Privacy	GEB_AVG_Disciplinair Onderzoek_versie 1.0.pdf	VIK	VIK-Intern onderzoek-disciplinair	Strafrechtelijke persoonsgegevens					x	2	5	10	Hoog	Issue: 5.1.2.i Risico: 5.1.2.i	5.1.2.i	IB risico	1-1-2024

Privacy	GEB_AVG_Disciplinair Onderzoek_versie 1.0.pdf	VIK	VIK-Intern onderzoek-disciplinair	Nationaliteit						3	4	12	Hoog	Issue: Van burgergetuigen wordt de nationaliteit genoteerd. Risico: Het risico bestaat dat op basis van nationaliteit discriminatie plaats vindt.	Stoppen met het vragen naar de nationaliteit. Dit kan door deze vraag uit het verslag burgergetuigen te schrappen.	IB risico	1-1-2024
Privacy	GEB_AVG_Disciplinair Onderzoek_versie 1.0.pdf	VIK	VIK-Intern onderzoek-disciplinair	IB-risicoanalyse op Delta						3	3	9	Midden	Issue: Er is een IB-risico analyse op Delta opgeleverd. Bij de implementatie en beoordeling van de risico's is (nog) onvoldoende gekeken naar de privacy risico's. Risico: o.a. onrechtmatige gegevensverwerking	Kijk opnieuw naar de uitkomsten van de IB-analyse en beoordeel de risico's voor de privacy van de categorieën betrokkenen. Neem in deze beoordeling ook de geaccepteerde risico's mee.	IB risico	1-1-2024
Privacy	GEB_AVG_Disciplinair Onderzoek_versie 1.0.pdf	VIK	VIK-Intern onderzoek-disciplinair	Er is te weinig privacy ondersteuning voor het VIK					x		3	3	9	Midden	Issue: Functionarissen kunnen niet altijd terecht bij een privacy adviseur met kennis van zaken van specifieke VIK gerelateerde privacyvraagstukken. Risico: Mogelijke onjuiste gegevensverwerking	Wijs een privacy adviseur aan met kennis van de VIK-processen die de VIKs kan ondersteunen.	IB risico	1-1-2024
Privacy	GEB_AVG_Disciplinair Onderzoek_versie 1.0.pdf	VIK	VIK-Intern onderzoek-disciplinair	Bewaartermijnen					x		4	3	12	Hoog	Issue: Bewaartermijn is wel bepaald, maar er wordt niet altijd naar gehandeld. Risico: De verwerking vindt langer plaats dan is toegestaan.	Regel beleid en werkprocessen in om de bewaartermijnen gestand te doen.	Werkproces gerelateerd	1-1-2024
Privacy	GEB_AVG_Disciplinair Onderzoek_versie 1.0.pdf	VIK	VIK-Intern onderzoek-disciplinair	Rechten van betrokkenen						x	4	3	12	Hoog	Issue: De betrokkene wordt niet volledig geïnformeerd conform de eisen van de AVG. De betrokkene kan de informatie niet makkelijk vinden. Risico: Betrokkene kan zijn rechten zoals inzage en rectificatie niet uitoefenen, omdat hij/zij geen weet heeft dat of in welke mate persoonsgegevens over hem/haar worden verwerkt.	Werk de brochure Intern Onderzoek bij en beschrijf daarin specifieker welke (categorieën) persoonsgegevens worden verwerkt. Geef daarbij ook specifiek aan waar de toepasselijke privacy statements op intranet / internet kunnen worden gevonden.	IB risico	1-1-2024
Privacy	GEB_AVG_Disciplinair Onderzoek_versie 1.0.pdf	VIK	VIK-Intern onderzoek-disciplinair	Kennis					x		2	4	8	Midden	Issue: De functionarissen zijn mogelijk onvoldoende op de hoogte van de privacy regels. Risico: Mogelijke onjuiste gegevensverwerking	Geef regelmatig zoveel mogelijk op de verwerking gerichte privacy training.	IB risico	1-1-2024
Privacy	GEB_AVG_Disciplinair Onderzoek_versie 1.0.pdf	VIK	VIK-Intern onderzoek-disciplinair	Discipline						x	3	3	9	Midden	Issue: Voor een uniforme werkwijze is het essentieel dat alle VIK-onderzoekers zich aan de gemaakte werkafspraken houden. Het is onzeker of dit voldoende gebeurt. Risico: Het risico bestaat dat de verwerking van persoonsgegevens niet conform de AVG geschiedt en de betrokkenen niet de bescherming hebben die de AVG aan hen biedt. Verder worden betrokkenen -medewerkers die onderwerp zijn van een disciplinair onderzoek-mogelijk ongelijk behandeld, als de aanpak van eenheden in de praktijk onvoldoende uniform is.	Teamchefs en coördinatoren moeten sturing geven zodanig dat de VIK-onderzoekers conform de werkafspraken werken (cultuurkwestie) Verricht steekproeven.	IB risico	1-1-2024
Privacy	GEB_AVG_Disciplinair Onderzoek_versie 1.0.pdf	VIK	VIK-Intern onderzoek-disciplinair	5.1.2.i							2	5	10	Hoog	Issue: 5.1.2.i Risico: 5.1.2.i	5.1.2.i	IB risico	1-1-2024
Privacy	GEB_AVG_Disciplinair Onderzoek_versie 1.0.pdf	VIK	VIK-Intern onderzoek-disciplinair	Gegevens derden						x	4	4	16	Hoog	Issue: Verwerking van persoonsgegevens van derden -dus personen die geen onderwerp zijn van een disciplinair onderzoek-, zonder dat daar noodzaak toe bestaat ("bijvangst"). Risico: Onrechtmatige gegevensverwerking, omdat niet aan het vereiste van minimale gegevensverwerking is voldaan. Verder is transparantie één van de kernwaarden van de AVG, maar deze derden hebben er geen weet van dat hun persoonsgegevens in de context van een disciplinair onderzoek zijn verwerkt.	Verwijder deze gegevens uit de onderzoeksdossiers of maak deze gegevens onleesbaar (blacklining).	IB risico	1-1-2024
Privacy	GEB_AVG_Disciplinair Onderzoek_versie 1.0.pdf	VIK	VIK-Intern onderzoek-disciplinair	5.1.2.i					x	x	3	4	12	Hoog	Issue 5.1.2.i Risico: 5.1.2.i	5.1.2.i	IB risico	1-1-2024
Privacy	GEB_AVG_Disciplinair Onderzoek_versie 1.0.pdf	VIK	VIK-Intern onderzoek-disciplinair	Opslag en verzending van gegevens				x	x	x	5	4	20	Zeer hoog	Issue: Er is geen maatwerksysteem waar alles in verwerkt en opgeslagen wordt. Daardoor bestaat er afhankelijkheid van opslag op netwerkschijven en verzending per e-mail. Risico: Niet in control zijn waar documenten zich bevinden. Documenten zouden kunnen gaan "rondslingeren" en langer worden bewaard dan toegestaan. Hierdoor neemt de kans toe op incidenten met betrekking tot de beschikbaarheid, integriteit of vertrouwelijkheid van persoonsgegevens.	Richt een maatwerksysteem in zodat VIK-medewerkers een dossier kunnen opbouwen in een veilige omgeving en veilig documenten kunnen delen.	IB risico	1-1-2024
Privacy	GEB_AVG_Disciplinair Onderzoek_versie 1.0.pdf	VIK	VIK-Intern onderzoek-disciplinair	Doorgifte themaregister						x	3	5	15	Hoog	Issue: Persoonsgegevens uit een disciplinair onderzoek worden mogelijk verstrekt aan het themaregister ambtelijke omkoping. Risico: Betrokkene wordt ten onrechte gelabeld met een profiel van "gevoelig voor / betrokken bij ambtelijke omkoping".	Volg het advies van 5.1.2.e en 5.1.2.e vastgelegd in het memo d.d. 10 maart 2021 over verstrekking van gegevens aan het themaregister. Dit memo is als bijlage 3 aan de GEB gehecht.	IB risico	1-1-2024
Privacy	GEB_AVG_Disciplinair Onderzoek_versie 1.0.pdf	VIK	VIK-Intern onderzoek-disciplinair	Bijzondere persoonsgegevens-uit hoorgesprek					x	x	3	4	12	Hoog	Issue: Er is geen wettelijke uitzondering voor: Bijzondere persoonsgegevens die: (i) medegedeeld zijn tijdens hoorgesprekken; én (ii) zijn vastgelegd (bijv. schriftelijk of elektronisch in een verslag of door middel van gespreksopname); én (iii) die niet noodzakelijk zijn ten behoeve van het onderzoek omdat niet aan het evidentie criterium is voldaan. Risico: Als deze gegevens worden gebruikt in het kader van disciplinaire onderzoeken, gebeurt dit in strijd met de AVG. Juist bijzondere persoonsgegevens worden extra beschermd in de AVG gezien hun gevoelige aard, dus schending van deze regels heeft een nadelige impact op de persoonlijke levenssfeer van een betrokkene.	Medewerkers instrueren zeer kritisch te zijn met het vermelden van bijzondere persoonsgegevens in de hoorverslagen. Als opname van gesprekken achterwege wordt gelaten, is er geen risico dat ten onrechte bijzondere persoonsgegevens "op band" komen te staan.	IB risico	1-1-2024
Privacy	GEB_AVG_Disciplinair Onderzoek_versie 1.0.pdf	VIK	VIK-Intern onderzoek-disciplinair	Bijzondere persoonsgegevens – open bronnen						x	3	4	12	Hoog	Issue: Er is geen wettelijke uitzondering: Bijzondere persoonsgegevens ontleend aan open bronnen die niet door de betrokkene zelf zijn openbaar gemaakt. Dit kan zowel gaan om bijzondere persoonsgegevens van de ambtenaar die onderwerp is van een disciplinair onderzoek als om bijzondere persoonsgegevens van derden. Risico: Als deze gegevens worden gebruikt in het kader van disciplinaire onderzoeken, gebeurt dit in strijd met de AVG. Juist bijzondere persoonsgegevens worden extra beschermd in de AVG gezien hun gevoelige aard, dus schending van deze regels heeft een nadelige impact op de persoonlijke levenssfeer van een betrokkene. Risico: Als deze gegevens worden gebruikt in het kader van disciplinaire onderzoeken, gebeurt dit in strijd met de AVG. Juist bijzondere persoonsgegevens worden extra beschermd in de AVG gezien hun gevoelige aard, dus schending van deze regels heeft een nadelige impact op de persoonlijke levenssfeer van een betrokkene.	Medewerkers instrueren zeer kritisch te zijn met het verzamelen van bijzondere persoonsgegevens.	IB risico	1-1-2024

Privacy	GEB_AVG_Disciplinair Onderzoek_versie 1.0.pdf	VIK	VIK-Intern onderzoek-disciplinair	Proportionaliteit en subsidiariteit					x	4	5	20	Zeer hoog	Issue: Besluitvorming over inzet middelen en daarmee het bepalen van aard en omvang van de te verwerken persoonsgegevens bij de uitvoering van een disciplinair onderzoek, ligt bij het bevoegd gezag. Ook bevoegd gezag dient zich aan AVG te houden en het is twijfelachtig of het bevoegd gezag voldoende instrumentarium heeft om dit te kunnen bepalen. Risico: Het risico bestaat dat de inzet van de onderzoeksmiddelen en daarmee de verwerking van persoonsgegevens niet conform de AVG geschiedt en de betrokkenen niet de bescherming hebben die de AVG aan hen biedt. Verder worden betrokkenen (medewerkers die onderwerp zijn van een disciplinair onderzoek) mogelijk ongelijk behandeld.	Disciplinaire onderzoeken onderverdelen in “klassen” van ernst van het vermoede plichtsverzuim en daarbij vermelden welke onderzoeksmiddelen in beginsel mogen worden ingezet; indien hiervan wordt afgeweken, kan het principe “comply or explain” gelden. Een duidelijk overzicht opstellen welke bronnen (applicaties / systemen) mogen worden geraadpleegd. Bevoegd gezag wint te allen tijde advies in bij een privacy adviseur. Evaluatie om te bepalen of de inzet van de onderzoeksmiddelen achteraf gezien proportioneel was. Doorvoeren van verbeterpunten n.a.v. evaluaties.	Werkproces gerelateerd	1-1-2024
Privacy	GEB_AVG_Disciplinair Onderzoek_versie 1.0.pdf	VIK	VIK-Intern onderzoek-disciplinair	Bewaartermijnen				x		4	3	12	Hoog	Issue: Bewaartermijn is wel bepaald, maar er wordt niet altijd naar gehandeld. Risico: De verwerking vindt langer plaats dan is toegestaan.	Regel beleid en werkprocessen in om de bewaartermijnen gestand te doen.	Werkproces gerelateerd	1-1-2024
Privacy	GEB_AVG_Disciplinair Onderzoek_versie 1.0.pdf	VIK	VIK-Intern onderzoek-disciplinair	Rechten van betrokkenen					x	4	3	12	Hoog	Issue: De betrokkene wordt niet volledig geïnformeerd conform de eisen van de AVG. De betrokkene kan de informatie niet makkelijk vinden. Risico: Betrokkene kan zijn rechten zoals inzage en rectificatie niet uitoefenen, omdat hij/zij geen weet heeft dat of in welke mate persoonsgegevens over hem/haar worden verwerkt.	Werk de brochure Intern Onderzoek bij en beschrijf daarin specifieker welke (categorieën) persoonsgegevens worden verwerkt. Geef daarbij ook specifiek aan waar de toepasselijke privacy statements op intranet / internet kunnen worden gevonden.	IB risico	1-1-2024
Privacy	GEB_AVG_Disciplinair Onderzoek_versie 1.0.pdf	VIK	VIK-Intern onderzoek-disciplinair	Er is te weinig privacy ondersteuning voor het VIK				x		3	3	9	Midden	Issue: Functionarissen kunnen niet altijd terecht bij een privacy adviseur met kennis van zaken van specifieke VIK gerelateerde privacyvraagstukken. Risico: Mogelijke onjuiste gegevensverwerking	Wijs een privacy adviseur aan met kennis van de VIK-processen die de VIKs kan ondersteunen.	IB risico	1-1-2024
Privacy	GEB_AVG_Disciplinair Onderzoek_versie 1.0.pdf	VIK	VIK-Intern onderzoek-disciplinair	Kennis				x		2	4	8	Midden	Issue: De functionarissen zijn mogelijk onvoldoende op de hoogte van de privacy regels. Risico: Mogelijke onjuiste gegevensverwerking	Geef regelmatig zoveel mogelijk op de verwerking gerichte privacy training.	IB risico	1-1-2024
Privacy	GEB_AVG_Disciplinair Onderzoek_versie 1.0.pdf	VIK	VIK-Intern onderzoek-disciplinair	Discipline					x	3	3	9	Midden	Issue: Voor een uniforme werkwijze is het essentieel dat alle VIK-onderzoekers zich aan de gemaakte werkafspraken houden. Het is onzeker of dit voldoende gebeurt. Risico: Het risico bestaat dat de verwerking van persoonsgegevens niet conform de AVG geschiedt en de betrokkenen niet de bescherming hebben die de AVG aan hen biedt. Verder worden betrokkenen -medewerkers die onderwerp zijn van een disciplinair onderzoek-mogelijk ongelijk behandeld, als de aanpak van eenheden in de praktijk onvoldoende uniform is.	Teamchefs en coördinatoren moeten sturing geven zodanig dat de VIK-onderzoekers conform de werkafspraken werken (cultuurkwestie) Verricht steekproeven.	IB risico	1-1-2024
Privacy	GEB_AVG_Disciplinair Onderzoek_versie 1.0.pdf	VIK	VIK-Intern onderzoek-disciplinair	5.1.2.i				x	x	2	5	10	Hoog	Issue: 5.1.2.i) Risico: 5.1.2.i	5.1.2.i	IB risico	1-1-2024
Privacy	GEB_AVG_Disciplinair Onderzoek_versie 1.0.pdf	VIK	VIK-Intern onderzoek-disciplinair	5.1.2.i						2	5	10	Hoog	Issue 5.1.2.i Risico 5.1.2.i	5.1.2.i .	IB risico	1-1-2024
Privacy	GEB_AVG_Disciplinair Onderzoek_versie 1.0.pdf	VIK	VIK-Intern onderzoek-disciplinair	5.1.2.i					x	4	5	20	Zeer hoog	Issue: 5.1.2.i Risico: 5.1.2.i	5.1.2.i	Werkproces gerelateerd	1-1-2024
Privacy	GEB_AVG_Disciplinair Onderzoek_versie 1.0.pdf	VIK	VIK-Intern onderzoek-disciplinair	5.1.2.i					x	3	4	12	Hoog	Issue: 5.1.2.i Risico: 5.1.2.i	5.1.2.i	IB risico	1-1-2024
Privacy	GEB_AVG_Disciplinair Onderzoek_versie 1.0.pdf	VIK	VIK-Intern onderzoek-disciplinair	Gegevens derden					x	4	4	16	Hoog	Issue: Verwerking van persoonsgegevens van derden -dus personen die geen onderwerp zijn van een disciplinair onderzoek-, zonder dat daar noodzaak toe bestaat (“bijvangst”). Risico: Onrechtmatige gegevensverwerking, omdat niet aan het vereiste van minimale gegevensverwerking is voldaan. Verder is transparantie één van de kernwaarden van de AVG, maar deze derden hebben er geen weet van dat hun persoonsgegevens in de context van een disciplinair onderzoek zijn verwerkt.	Verwijder deze gegevens uit de onderzoeksdossiers of maak deze gegevens onleesbaar (blacklining).	IB risico	1-1-2024
Privacy	GEB_AVG_Disciplinair Onderzoek_versie 1.0.pdf	VIK	VIK-Intern onderzoek-disciplinair	Bijzondere persoonsgegevens-uit hoorgesprek			x		x	3	4	12	Hoog	Issue: Er is geen wettelijke uitzondering voor: Bijzondere persoonsgegevens die: (i) medegedeeld zijn tijdens hoorgesprekken; én (ii) zijn vastgelegd (bijv. schriftelijk of elektronisch in een verslag of door middel van gespreksopname); én (iii) die niet noodzakelijk zijn ten behoeve van het onderzoek omdat niet aan het evidentie criterium is voldaan. Risico: Als deze gegevens worden gebruikt in het kader van disciplinaire onderzoeken, gebeurt dit in strijd met de AVG. Juist bijzondere persoonsgegevens worden extra beschermd in de AVG gezien hun gevoelige aard, dus schending van deze regels heeft een nadelige impact op de persoonlijke levenssfeer van een betrokkene.	Medewerkers instrueren zeer kritisch te zijn met het vermelden van bijzondere persoonsgegevens in de hoorverslagen. Als opname van gesprekken achterwege wordt gelaten, is er geen risico dat ten onrechte bijzondere persoonsgegevens "op band” komen te staan.	IB risico	1-1-2024

Privacy	GEB_AVG_Disciplinair Onderzoek_versie 1.0.pdf	VIK	VIK-Intern onderzoek-disciplinair	Bijzondere persoonsgegevens – open bronnen					x	3	4	12	Hoog	Issue: Er is geen wettelijke uitzondering: Bijzondere persoonsgegevens ontleend aan open bronnen die niet door de betrokkene zelf zijn openbaar gemaakt. Dit kan zowel gaan om bijzondere persoonsgegevens van de ambtenaar die onderwerp is van een disciplinair onderzoek als om bijzondere persoonsgegevens van derden. Risico: Als deze gegevens worden gebruikt in het kader van disciplinaire onderzoeken, gebeurt dit in strijd met de AVG. Juist bijzondere persoonsgegevens worden extra beschermd in de AVG gezien hun gevoelige aard, dus schending van deze regels heeft een nadelige impact op de persoonlijke levenssfeer van een betrokkene. Risico: Als deze gegevens worden gebruikt in het kader van disciplinaire onderzoeken, gebeurt dit in strijd met de AVG. Juist bijzondere persoonsgegevens worden extra beschermd in de AVG gezien hun gevoelige aard, dus schending van deze regels heeft een nadelige impact op de persoonlijke levenssfeer van een betrokkene.	Medewerkers instrueren zeer kritisch te zijn met het verzamelen van bijzondere persoonsgegevens.	IB risico	1-1-2024	
Privacy	GEB_AVG_Disciplinair Onderzoek_versie 1.0.pdf	VIK	VIK-Intern onderzoek-disciplinair	Bijzondere persoonsgegevens:gezondheidsgegevens				x		x	4	3	12	Hoog	Issue: Er is geen wettelijke uitzondering voor: Gezondheidsgegevens: (ii) of men medicijnen of andere middelen gebruikt die invloed kunnen hebben op het hoorgesprek met de VIK-onderzoeker (staat in standaard hoorverslag). Risico: Als deze gegevens worden gebruikt in het kader van disciplinaire onderzoeken, gebeurt dit in strijd met de AVG. Juist bijzondere persoonsgegevens worden extra beschermd in de AVG gezien hun gevoelige aard, dus schending van deze regels heeft een nadelige impact op de persoonlijke levenssfeer van een betrokkene.	Deze vraag achterwege vragen in het hoorverslag. Er wordt al in meer algemene termen gevraagd of men in staat is aan het gesprek deel te nemen.	IB risico	1-1-2024	
Privacy	GEB_AVG_Disciplinair Onderzoek_versie 1.0.pdf	VIK	VIK-Intern onderzoek-disciplinair	Bijzondere persoonsgegevens:lidmaatschap vakbond					x		2	2	4	Midden	Issue: Lidmaatschap vakbond: indien een betrokkene zich laat bijstaan door een gemachtigde/jurist verbonden aan een vakbond en dit wordt vastgelegd, worden daarmee gegevens van betrokkene over lidmaatschap van een vakbond verwerkt. Lidmaatschap vakbond is een bijzonder persoonsgegeven en er kan geen beroep worden gedaan op een wettelijke uitzondering om dit bijzondere persoonsgegeven te mogen verwerken. Risico: Als deze gegevens worden verwerkt in het kader van disciplinaire onderzoeken, gebeurt dit in strijd met de AVG.	Lidmaatschap vakbond wordt in Nederland in het algemeen niet als zeer kritisch ervaren. Daarom kan in dit risico worden voorzien door tijdens het hoorgesprek uitdrukkelijke toestemming te vragen voor vermelding hiervan en dit in het verslag op te nemen. Indien geen toestemming wordt gegeven, dan vermelding achterwege laten.	IB risico	1-1-2024	
Privacy	GEB_AVG_Disciplinair Onderzoek_versie 1.0.pdf	VIK	VIK-Intern onderzoek-disciplinair	5.1.2.i					x	2	5	10	Hoog	Issue: 5.1.2.i Risico: 5.1.2.i	5.1.2.i	IB risico	1-1-2024	
Privacy	GEB_AVG_Disciplinair Onderzoek_versie 1.0.pdf	VIK	VIK-Intern onderzoek-disciplinair	5.1.2.i				x	x	3	4	12	Hoog	Issue 5.1.2.i	5.1.2.i	IB risico	1-1-2024	
Privacy	GEB_AVG_Disciplinair Onderzoek_versie 1.0.pdf	VIK	VIK-Intern onderzoek-disciplinair	Nationaliteit						3	4	12	Hoog	Issue: Van burgergetuigen wordt de nationaliteit genoteerd. Risico: Het risico bestaat dat op basis van nationaliteit discriminatie plaats vindt.	Stoppen met het vragen naar de nationaliteit. Dit kan door deze vraag uit het verslag burgergetuigen te schrappen.	IB risico	1-1-2024	
Privacy	GEB_AVG_Disciplinair Onderzoek_versie 1.0.pdf	VIK	VIK-Intern onderzoek-disciplinair	Opslag en verzending van gegevens				x	x	x	5	4	20	Zeer hoog	Issue: Er is geen maatwerksysteem waar alles in verwerkt en opgeslagen wordt. Daardoor bestaat er afhankelijkheid van 5.1.2.i Risico: Niet in control zijn waar documenten zich bevinden. Documenten zouden kunnen 5.1.2.i en langer worden bewaard dan toegestaan. Hierdoor neemt de kans toe op incidenten met betrekking tot 5.1.2.i	Richt een maatwerksysteem in zodat VIK-medewerkers een dossier kunnen opbouwen in een veilige omgeving en veilig documenten kunnen delen.	IB risico	1-1-2024	
Privacy	GEB_AVG_Disciplinair Onderzoek_versie 1.0.pdf	VIK	VIK-Intern onderzoek-disciplinair	IB-risicoanalyse op Delta						3	3	9	Midden	Issue: Er is een IB-risico analyse op Delta opgeleverd. Bij de implementatie en beoordeling van de risico's is (nog) onvoldoende gekeken naar de privacy risico's. Risico: o.a. onrechtmatige gegevensverwerking	Kijk opnieuw naar de uitkomsten van de IB-analyse en beoordeel de risico's voor de privacy van de categorieën betrokkenen. Neem in deze beoordeling ook de geaccepteerde risico's mee.	IB risico	1-1-2024	
Privacy	GEB_AVG_Disciplinair Onderzoek_versie 1.0.pdf	VIK	VIK-Intern onderzoek-disciplinair	Doorgifte themaregister					x	3	5	15	Hoog	Issue: Persoonsgegevens uit een disciplinair onderzoek worden mogelijk verstrekt aan het themaregister ambtelijke omkoping. Risico: Betrokkene wordt ten onrechte gelabeld met een profiel van "gevoelig voor / betrokken bij ambtelijke omkoping".	Volg het advies van 5.1.2.e en 5.1.2.e vastgelegd in het memo d.d. 10 maart 2021 over verstrekking van gegevens aan het themaregister. Dit memo is als bijlage 3 aan de GEB gehecht.	IB risico	1-1-2024	
Privacy	20231030 GEB Vermissingen. 1.0.docx	GGP	Vermissing	Werkproces						4	2	8	Midden	De verwerking heeft een verouderd werkproces in de bedrijfsarchitectuur. Er staan nog subverwerkingen in benoemd die niet meer bestaan. Deze kunnne uit de bedrijfsarchitectuur verwijderd worden.	De directie operatien heeft een opdracht nodig van de portefeuillehouder om de werkprocessen te blijven actualiseren. Inventariseer de mate van diversiteit van de verwerkingen en stel het beveiligings- en privacyrisico's vast. Stel een protocol op om een uniforme verwerking te realiseren.	Werkproces gerelateerd	1-1-2024	30-jun-23
Privacy	20231030 GEB Vermissingen. 1.0.docx	GGP	Vermissing	Werkproces						3	2	6	Midden	De verwerking wordt in de eenheden niet volledig uniform uitgevoerd.	Zorg voor uniforme werkwijze met controle momenten.	IB risico	1-1-2024	
Privacy	20231030 GEB Vermissingen. 1.0.docx	GGP	Vermissing	Autorisatie					x	4	3	12	Hoog	De autorisaties voor deze verwerking worden niet periodiek/regelmatig gecontroleerd	Zorg voor een reguliere controle van de autorisaties.	IB risico	1-1-2024	
Privacy	20231030 GEB Vermissingen. 1.0.docx	GGP	Vermissing	Verwerkingstermijnen						5	3	15	Hoog	De verwerkingstermijnen worden niet altijd nageleefd waardoor de verwerking langer plaatsvindt en de gegevens langer toegankelijk zijn dan is toegestaan. Dit geldt met name voor de bestanden die via e-mail verzonden worden.	Pas systemen en procedures aan om de verwerkingstermijnen na te leven. Geef de medewerkers de nodige instructies om ook bijvoorbeeld de mailboxen op te schonen.	IB risico	1-1-2024	30-jun-23

Privacy	GEB HAVANK4CATCH2 2023.pdf	Specialistische Opsporing	Gelaatsvergelijking	Onbekend			x	x	x	2	3	6	Midden	Onjuiste verkrijging van biometriegegevens in de databank heeft gevolgen voor de rechten en vrijheid van de betrokkene. 1. De verkregen biometriegegevens voldoen net aan de eisen voor opname in de databank 2. De aanvraag voldoet niet aan de gestelde eisen / is onrechtmatig 3. De status van de verdacht is veranderd in gewezen verdachte en deze verandering is niet doorgevoerd in de databank 4. De bewaartermijn is van de opgeslagen gegevens in de databank is verstreken of de gegevens hadden geschoond moeten worden 5. Het refenrentiebestand/gegevens mogen niet gebruikt worden 6. Verkeerde match en/of verkeerde menselijke expert conclusie (fout positief/fout negatief)	Zie document "GEB HAVANK4CATCH2 2023.pdf" voor een uitgebreide beschrijving van de maatregelen	IB risico	1-1-2024	
Privacy	GEB HAVANK4CATCH2 2023.pdf	Specialistische Opsporing	Gelaatsvergelijking	Onbekend			x		x	3	4	12	Hoog	Er is een datalek opgetreden waardoor gegevens toegankelijk zijn voor onbevoegden 7. Lek in het aanvraagproces 8. De opgeslagen aanvragen zijn toegankelijk 9. Lek in de databank 10. Lek in het rapportageproces 11. De opgeslagen rapportages zijn toegankelijk	Zie document "GEB HAVANK4CATCH2 2023.pdf" voor een uitgebreide beschrijving van de maatregelen	IB risico	1-1-2024	1-apr-23
Privacy	GEB HAVANK4CATCH2 2023.pdf	Specialistische Opsporing	Gelaatsvergelijking	Onbekend					x	1	4	4	Midden	Datalek of gijzeling gegevens (ransomware) 12. Geavanceerde dreiging door statelijke actore, georganiseerde crimilaliteit of hacktivisten	Zie document "GEB HAVANK4CATCH2 2023.pdf" voor een uitgebreide beschrijving van de maatregelen	IB risico	1-1-2024	
Privacy	GEB HAVANK4CATCH2 2023.pdf	Specialistische Opsporing	Gelaatsvergelijking	Onbekend			x			3	3	9	Midden	De mogelijkheden om de biometriegegevens te verwerken nemen toe. De wetgeving kan hierop aangepast worden. 13. Er zijn steeds meer camera's en opslagmedia (telefoons, dataschijven etc) in de samenleving en mogelijkheden voorgelaatsherkenning nemen toe. De wetgeving is specifiek over verwerken en vergelijken van vingerafdrukken. Voor gelaatsherkenning is het vergelijken minder specifiek beschreven.	Zie document "GEB HAVANK4CATCH2 2023.pdf" voor een uitgebreide beschrijving van de maatregelen	IB risico	1-1-2024	
Privacy	GEB Opnemen aangifte versie 1.0, 20-09-2023 .pdf	GGP	Opnemen aangifte	Uitvoering						3	3	9	Midden	Issue: De verwerking wordt in de eenheden niet uniform uitgevoerd. Risico: De verwerking is niet transparant; verwerking is niet beheersbaar als op verschillende locaties verschillende werkwijzen worden gehanteerd.	Stel landelijke richtlijnen en protocollen over de gegevensverwerking op en controleer deze regelmatig.	IB risico	1-1-2024	
Privacy	GEB Opnemen aangifte versie 1.0, 20-09-2023 .pdf	GGP	Opnemen aangifte	Autorisaties					x	3	3	9	Midden	Issue: Autorisaties worden niet periodiek gecontroleerd. Risico: 5.1.2.i [redacted]	Controleer de autorisaties regelmatig 5.1.2.i [redacted]	IB risico	1-1-2024	1-apr-23
Privacy	GEB Opnemen aangifte versie 1.0, 20-09-2023 .pdf	GGP	Opnemen aangifte	Verwerkingstermijnen en bewaartermijnen				x		5	3	15	Hoog	Issue: De verwerkingstermijnen en bewaartermijnen worden niet nageleefd, waardoor de verwerking langer plaatsvindt en de gegevens langer toegankelijk zijn dan wettelijk is toegestaan. Risico: o.a. onrechtmatige gegevensverwerking.	Pas systemen en procedures aan om de verwerkingstermijnen en bewaartermijnen na te leven.	IB risico	1-1-2024	1-apr-23
Privacy	GEB Opnemen aangifte versie 1.0, 20-09-2023 .pdf	GGP	Opnemen aangifte	Verwerkingstermijnen en bewaartermijnen zijn niet inzichtelijk				x		5	4	20	Zeer hoog	Issue: Verwerkingstermijnen en bewaartermijnen zijn bij gebruik van (privé) e-mail, WhatsApp en netwerkschijven onvoldoende inzichtelijk en daardoor niet beheersbaar. Risico: o.a. onrechtmatige verwerking, de verwerking is niet beheersbaar en bewaartermijnen kunnen niet worden gewaarborgd.	Stuur op juist gebruik middels en voer controles in op netwerkschijven om de verwerkingstermijnen en bewaartermijnen na te leven.	IB risico	1-1-2024	1-apr-23
Privacy	GEB Opnemen aangifte versie 1.0, 20-09-2023 .pdf	GGP	Opnemen aangifte	Downloads vanuit BVH				x	x	5	3	15	Hoog	Issue: Om een onderzoeksdossier op te maken dient er te worden gedownload vanuit BVH. 5.1.2.i [redacted] De verwerking is hierdoor niet beheersbaar en bewaartermijnen kunnen niet worden gewaarborgd. Risico: datalek, niet voldoen aan de wettelijke vereisten	Voorkom dat downloaden kan en noodzakelijk is of stel een policy in, waarbij de downloads van medewerkers periodiek opgeschoond worden.	IB risico	1-1-2024	
Privacy	GEB Opnemen aangifte versie 1.0, 20-09-2023 .pdf	GGP	Opnemen aangifte	Kennis				x	x	3	3	9	Midden	Issue: Medewerkers zijn onvoldoende op de hoogte van de privacyregels, dit blijkt onder andere uit onjuist middelen- en systemengebruik. Risico: o.a. datalekken	Geef regelmatig privacy training. Denk hierbij aan het volgen van een training op het gebied van privacy awareness.	IB risico	1-1-2024	
Privacy	GEB Opnemen aangifte versie 1.0, 20-09-2023 .pdf	GGP	Opnemen aangifte	Onjuist gebruik middelen			x		x	5	4	20	Zeer hoog	Issue: De beschikbaar gestelde tools worden niet gebruikt om het toe te voegen bewijsmateriaal te verkrijgen binnen de digitale infrastructuur van de politie. Risico: o.a. datalekken	Onderzoek de mogelijkheden voor eenvoudigere gegevensdeling met burgers.	IB risico	1-1-2024	
Privacy	GEB Opnemen aangifte versie 1.0, 20-09-2023 .pdf	GGP	Opnemen aangifte	Inzet privé middelen					x	5	4	20	Zeer hoog	Issue: Medewerkers gebruiken (privé) Whatsapp voor het verkrijgen van documenten/foto's die kunnen dienen als bewijsmateriaal. Deze worden vervolgens via privé e-mail overgeheveld naar de politieomgeving. Risico: o.a. datalekken	Zie toe op gebruik van de applicatie Bestandsuitwisseling en pas de applicatie waar nodig aan zodat het makkelijker in het gebruik is.	IB risico	1-1-2024	
Privacy	GEB Opnemen aangifte versie 1.0, 20-09-2023 .pdf	GGP	Opnemen aangifte	Bijzondere politiegegevens						3	3	9	Midden	Issue: Er ontbreken concrete werkinstructies over de omgang met bijzondere politiegegevens in het kader van deze verwerking. Risico: onrechtmatige verwerking	Stel heldere werkinstructies op en instrueer de collega's	Werkproces gerelateerd	1-1-2024	1-apr-23
Privacy	GEB Opnemen aangifte versie 1.0, 20-09-2023 .pdf	GGP	Opnemen aangifte	Proportionaliteit en subsidiariteit					x	5	3	15	Hoog	Issue: Medewerkers kunnen meer gegevens inzien dan noodzakelijk voor de uitoefening van hun taak Risico: datalekken en onrechtmatige gegevensverwerking die niet voldoet aan proportionaliteit en subsidiariteit.	Beperk de beschikbare gegevens tot de gegevens die noodzakelijk zijn voor de uitoefening van de taak van de medewerkers	IB risico	1-1-2024	1-apr-23
Privacy	GEB Opnemen aangifte versie 1.0, 20-09-2023 .pdf	GGP	Opnemen aangifte	5.1.2.i [redacted]					x	5	3	15	Hoog	Issue: 5.1.2.i [redacted] Risico: 5.1.2.i [redacted]	5.1.2.i [redacted]	IB risico	1-1-2024	1-apr-23
Privacy	GEB Opnemen aangifte versie 1.0, 20-09-2023 .pdf	GGP	Opnemen aangifte	Gegevens-verstrekking						2	2	4	Midden	Issue: Gegevensverstrekking gebeurt via een geautomatiseerd proces. Risico: onrechtmatige verstrekking	Controleer regelmatig of de verstrekkingen (technisch) juist worden uitgevoerd.	IB risico	1-1-2024	
Privacy	20231130 GEB WPG - Behandelen M-Melding - versie 1.0.pdf	Intelligence	Behandelen M-melding	Bedrijfsreferentiemodel is sterk verouderd						2	3	6	Midden	Issue: Bedrijfsreferentiemodel is sterk verouderd. Risico: Het proces van de verwerking is niet adequaat in kaart gebracht. Hierdoor is de verwerking niet voldoende beheersbaar.	Actualiseer het bedrijfsreferentiemodel (BRM).	IB risico	1-1-2024	

Privacy	20231130 GEB WPG - Behandelen M-Melding - versie 1.0.pdf	Intelligence	Behandelen M-melding	Autorisaties					x	5	3	15	Hoog	Issue: Autorisaties die verleend zijn via [redacted] worden niet altijd periodiek gecontroleerd. Risico: [redacted]	Controleer de autorisaties regelmatig [redacted]	IB risico	1-1-2024
Privacy	20231130 GEB WPG - Behandelen M-Melding - versie 1.0.pdf	Intelligence	Behandelen M-melding	Mens						5	3	15	Hoog	Issue: Onvoldoende zicht op of verwerkingstermijnen bij inzet e-mail en netwerkschijven. Risico: o.a. onrechtmatige gegevensverwerking.	Instrueer medewerkers en draag zorg voor privacy awareness.	IB risico	1-1-2024
Privacy	20231130 GEB WPG - Behandelen M-Melding - versie 1.0.pdf	Intelligence	Behandelen M-melding	Verwerkingstermijnen						5	3	15	Hoog	Issue: Onvoldoende zicht op of verwerkingstermijnen bij inzet e-mail en netwerkschijven. Risico: o.a. onrechtmatige gegevensverwerking.	Pas systemen en procedures aan om de verwerkingstermijnen en na te leven.	IB risico	1-1-2024
Privacy	20231130 GEB WPG - Behandelen M-Melding - versie 1.0.pdf	Intelligence	Behandelen M-melding	Verwerkingstermijnen						5	3	15	Hoog	Issue: Formeel gezien voldoen we niet aan de vernietigingstermijnen zoals vastgesteld in de Wpg. Risico: o.a. onrechtmatige gegevensverwerking.	Er zijn geen mogelijke maateregelen vanwege het besluit van de korpschef. De korpschef heeft besloten politiegegevens niet standaard te vernietigen als de bewaartermijn op grond van de Wpg is verstreken in verband met de opsporing van cold cases.	IB risico	1-1-2024
Privacy	GEB Opnemen Vertrouwelijke Communicatie versie 1.0, 20-11-2023.pdf	Specialistische Opsporing	Opnemen Vertrouwelijke Communicatie	Bewaar- en vernietigingstermijnen					x	4	3	12	Hoog	Issue: Een onderzoeksdossier wordt door de opsporingsambtenaar van politie in de praktijk pas op afgehandeld gezet na een afdoeningsbericht van het OM. Doordat dit proces niet is geautomatiseerd en/of een afdoeningsbericht structureel achterwege blijft, komt het in de praktijk veelvuldig voor dat dossiers met daarin politiegegevens blijven staan op status “verwerken” en daardoor gegevens langer worden verwerkt dan wettelijk is toegestaan. Risico: Politiegegevens worden langer verwerkt dan de wettelijke termijnen waardoor er langer dan is toegestaan inbreuk wordt gemaakt op de privacy van betrokkenen. Hierdoor kan er imagoschade optreden of kan de politie een last onder bestuursdwang of bestuurlijke boete opgelegd krijgen van de Autoriteit Persoonsgegevens (AP) en andere onderzoeken die starten met deze gegevens kunnen een onrechtmatig basis hebben.	Inventariseer in hoeverre wordt voldaan aan de wettelijke bewaar- en vernietigings-termijnen en pak de geconsta-teerde afwijkingen op. Maak afspraken met het OM over tijdige (bij voorkeur geautoma-tiseerde) kennisgeving met betrekking tot het sluiten van een dossier, zodat de wettelijke bewaar- en vernietigings-termijnen gaan lopen. Richt vervolgens een eigen geautoma-tiseerd proces in met betrekking tot de bewaar- en vernietigings-termijnen.	IB risico	1-1-2024
Privacy	GEB Opnemen Vertrouwelijke Communicatie versie 1.0, 20-11-2023.pdf	Specialistische Opsporing	Opnemen Vertrouwelijke Communicatie	Bewaar- en vernietigingstermijnen			x	x	x	4	3	12	Hoog	Issue: Politiegegevens die in Summ-IT worden opgeslagen worden niet vernietigd. Daarnaast is er geen bewaartermijn met beperkte toegankelijkheid ingericht en zijn er geen poortwachters aangesteld. Risico: Politiegegevens zijn hierdoor onvoldoende beschermd en worden langer verwerkt dan de wettelijke termijnen waardoor er sprake is van een onrechtmatige verwerking. Als gevolg hiervan wordt er langer dan is toegestaan inbreuk gemaakt op de privacy van betrokkenen. Hierdoor kan er imagoschade optreden of kan de politie een last onder bestuursdwang of bestuurlijke boete opgelegd krijgen van de Autoriteit Persoonsgegevens (AP) en andere onderzoeken die starten met deze gegevens een onrechtmatig basis hebben.	Vernietig politie-gegevens die in Summ-IT staan waarvan de bewaartermijn is verstreken.	IB risico	1-1-2024
Privacy	GEB Doorzoeking plaats delict.pdf	Generieke Opsporing	Doorzoeking plaats delict	Bewaar- en vernietigingstermijnen					x	4	3	12	Hoog	Issue: Een onderzoeksdossier wordt door de opsporingsambtenaar van politie in de praktijk pas op afgehandeld gezet na een afdoeningsbericht van het OM. Doordat dit proces niet is geautomatiseerd en/of een afdoeningsbericht structureel achterwege blijft, komt het in de praktijk veelvuldig voor dat dossiers met daarin politiegegevens blijven staan op status “verwerken” en daardoor gegevens langer worden verwerkt dan wettelijk is toegestaan. Risico: Politiegegevens worden langer verwerkt dan de wettelijke termijnen waardoor er langer dan is toegestaan inbreuk wordt gemaakt op de privacy van betrokkenen. Hierdoor kan er imagoschade optreden of kan de politie een last onder bestuursdwang of bestuurlijke boete opgelegd krijgen van de Autoriteit Persoonsgegevens (AP) en andere onderzoeken die starten met deze gegevens een onrechtmatig basis hebben.	Inventariseer in hoeverre wordt voldaan aan de wettelijke bewaar- en vernietigings-termijnen en pak de geconsta-teerde afwijkingen op. Maak afspraken met het OM over tijdige (bij voorkeur geautoma-tiseerde) kennisgeving met betrekking tot het sluiten van een dossier, zodat de wettelijke bewaar- en vernietigings-termijnen gaan lopen. Richt vervolgens een eigen geautoma-tiseerd proces in met betrekking tot de bewaar- en vernietigings-termijnen.	IB risico	1-1-2024
Privacy	GEB Doorzoeking plaats delict.pdf	Generieke Opsporing	Doorzoeking plaats delict	Bewaar- en vernietigingstermijnen					x	4	3	12	Hoog	Issue: Momenteel worden politiegegevens die in het politiesysteem BVH staan niet structureel vernietigd. Risico: [redacted]	[redacted]	IB risico	1-1-2024
Privacy	GEB Doorzoeking plaats delict.pdf	Generieke Opsporing	Doorzoeking plaats delict	Bewaar- en vernietigingstermijnen										Issue: [redacted]			
Privacy	GEB Doorzoeking plaats delict.pdf	Generieke Opsporing	Doorzoeking plaats delict	Bewaar- en vernietigingstermijnen			x	x	x	4	3	12	Hoog	Risico: [redacted]	Vernietig politie-gegevens die in [redacted] staan waarvan de bewaartermijn is verstreken.	IB risico	1-1-2024
Privacy	GEB Doorzoeking plaats delict.pdf	Generieke Opsporing	Doorzoeking plaats delict	Bewaar- en vernietigingstermijnen			x			4	5	20	Zeer hoog	Issue: [redacted]. Risico: [redacted]	[redacted]	IB risico	1-1-2024

Privacy	GEB Wpg-Huiselijk geweld en kindermishandeling versie 1, 21-11-2023.pdf	Zorg & Veiligheid	Huiselijk geweld / kindermishandeling	Uitvoering						5	3	15	Hoog	Issue: De verwerking wordt in de eenheden niet uniform uitgevoerd. Risico: De verwerking is niet transparant; verwerking is niet beheersbaar als op verschillende locaties verschillende werkwijzen worden gehanteerd.	Onderzoek hoe de landelijke uniformiteit kan worden verbeterd. Bijvoorbeeld door: - Controleer de landelijke werkinstructies op naleving. - Pas waar nodig werkinstructies aan. - Actualiseer het BRM.	Werkproces gerelateerd	1-1-2024
Privacy	GEB Wpg-Huiselijk geweld en kindermishandeling versie 1, 21-11-2023.pdf	Zorg & Veiligheid	Huiselijk geweld / kindermishandeling	Autorisaties					x	5	3	15	Hoog	Issue: Autorisaties worden niet periodiek gecontroleerd. Risico: Medewerkers kunnen meer gegevens inzien dan noodzakelijk voor de uitoefening van hun taak; datalekken en onrechtmatig gegevensgebruik.	Controleer de autorisaties regelmatig om te voorkomen dat medewerkers meer gegevens inzien dan noodzakelijk is voor de uitoefening van hun taak	IB risico	1-1-2024
Privacy	GEB Wpg-Huiselijk geweld en kindermishandeling versie 1, 21-11-2023.pdf	Zorg & Veiligheid	Huiselijk geweld / kindermishandeling	Verwerkingstermijnen						5	3	15	Hoog	Issue: Door inzet van e-mail en netwerkschijven is er onvoldoende zicht op of verwerkingstermijnen, waardoor de verwerking mogelijk langer plaatsvindt en de gegevens mogelijk langer toegankelijk zijn dan wettelijk is toegestaan. Risico: o.a. onrechtmatige gegevensverwerking.	Pas systemen en procedures aan om de verwerkingstermijnen en bewaartermijnen na te leven.	IB risico	1-1-2024
Privacy	GEB Wpg-Huiselijk geweld en kindermishandeling versie 1, 21-11-2023.pdf	Zorg & Veiligheid	Huiselijk geweld / kindermishandeling	Vernietigingstermijnen						5	3	15	Hoog	Issue: Formeel gezien voldoen we niet aan de vernietigingstermijnen zoals vastgesteld in de WPG. Risico: o.a. onrechtmatige gegevensverwerking.	Er zijn geen mogelijke maatregelen. De korpschef heeft besloten politiegegevens niet standaard te vernietigen als de bewaartermijn op grond van de Wpg is verstreken in verband met de opsporing van cold cases.	IB risico	1-1-2024
Privacy	GEB Wpg-Huiselijk geweld en kindermishandeling versie 1, 21-11-2023.pdf	Zorg & Veiligheid	Huiselijk geweld / kindermishandeling	Big Data verwerking is niet getoetst aan Kwaliteitskader Big Data					x	5	3	15	Hoog	Issue: [redacted] Risico [redacted]	[redacted] .	IB risico	1-1-2024
Privacy	GEB Wpg-Huiselijk geweld en kindermishandeling versie 1, 21-11-2023.pdf	Zorg & Veiligheid	Huiselijk geweld / kindermishandeling	EBO Ms Acces Database						5	3	15	Hoog	Issue: [redacted] Risico: [redacted]	[redacted] Controleer of er binnen andere eenheden ook dergelijke databases worden gebruikt.	IB risico	1-1-2024
Privacy	GEB Wpg-Huiselijk geweld en kindermishandeling versie 1, 21-11-2023.pdf	Zorg & Veiligheid	Huiselijk geweld / kindermishandeling	Gegevens-verstrekking					x	3	5	15	Hoog	Issue: Binnen deze verwerking vinden veel verstrekkingen plaats. Vanuit het onderzoek en de gesprekken is het beeld ontstaan dat de noodzakelijkheid van de verstrekking niet altijd wordt afgewogen. Er wordt vaak gekozen om de mutaties in zijn geheel te verstrekken i.p.v. alleen de relevante onderdelen. Risico: o.a. onrechtmatige gegevensverstrekking, kans op datalekken.	Instrueer medewerkers dat de noodzakelijkheid van de verstrekkingen per casus beoordeeld dient te worden en neem dit waar mogelijk op in werkinstructies. Controleer daarnaast periodiek welke gegevens verstrekt worden aan de verschillende ketenpartners.	Werkproces gerelateerd	1-1-2024
Privacy	20231201 GEB Wpg - Uitvoeren Onderzoek Publiek Toegankelijke Bronnen - versie 0.2.docx	Intelligence	Uitvoeren onderzoek publiek toegankelijke bronnen	Werkproces						3	3	9	Midden	Issue: De verwerking heeft een verouderd werkproces in het bedrijfsreferentiemodel en is niet compleet beschreven. Risico: De verwerking is niet transparant; mogelijk worden er verschillende werkwijzen gehanteerd.	Zorg dat de werkprocessen geactualiseerd worden en centraal worden vastgesteld.	Werkproces gerelateerd	1-1-2024
Privacy	20231201 GEB Wpg - Uitvoeren Onderzoek Publiek Toegankelijke Bronnen - versie 0.2.docx	Intelligence	Uitvoeren onderzoek publiek toegankelijke bronnen	Autorisaties					x	5	3	15	Hoog	Issue: Er is onvoldoende zicht op of toegekende autorisaties aansluiten op het opleidingsniveau en de taak van OSINT-medewerkers. Risico: Medewerkers kunnen meer middelen inzetten dan passend is bij de uitoefening van hun taak; onrechtmatige verkrijging gegevens	Controleer de autorisaties regelmatig om te zorgen dat beschikbare middelen passend zijn bij de taak en het opleidingsniveau.	IB risico	1-1-2024
Privacy	20231201 GEB Wpg - Uitvoeren Onderzoek Publiek Toegankelijke Bronnen - versie 0.2.docx	Intelligence	Uitvoeren onderzoek publiek toegankelijke bronnen	Verwerkingstermijnen en bewaartermijnen zijn niet inzichtelijk				x		5	3	15	Hoog	Issue: Verwerkingstermijnen en bewaartermijnen zijn bij gebruik van e-mail en netwerkschijven onvoldoende inzichtelijk en daardoor niet beheersbaar. Risico: o.a. onrechtmatige verwerking, de verwerking is niet beheersbaar en bewaartermijnen kunnen niet worden gewaarborgd.	Onderzoek of/welke oplossing mogelijk is voor het naleven van de verwerkings-en vernietigingstermijnen voor gegevens in Outlook en op netwerkschijven.	IB risico	1-1-2024
Privacy	20231201 GEB Wpg - Uitvoeren Onderzoek Publiek Toegankelijke Bronnen - versie 0.2.docx	Intelligence	Uitvoeren onderzoek publiek toegankelijke bronnen	Adresseren OSINT-vraagstukken						3	3	9	Midden	Issue: [redacted] Risico: o.a. onrechtmatige verkrijging en verwerking van gegevens.	Maak inzichtelijk welke afdelingen/medewerkers kunnen worden ingezet bij [redacted] -vraagstukken.	IB risico	1-1-2024
Privacy	20231201 GEB Wpg - Uitvoeren Onderzoek Publiek Toegankelijke Bronnen - versie 0.2.docx	Intelligence	Uitvoeren onderzoek publiek toegankelijke bronnen	Signalering naar andere afdelingen				x		5	3	15	Hoog	Issue: [redacted] Risico: [redacted]	Stel werkinstructies op waarin richtlijnen worden gegeven over wanneer er een signaal naar een andere afdeling wordt gegeven.	Werkproces gerelateerd	1-1-2024
Privacy	20231201 GEB Wpg - Uitvoeren Onderzoek Publiek Toegankelijke Bronnen - versie 0.2.docx	Intelligence	Uitvoeren onderzoek publiek toegankelijke bronnen	Rechtmatige verkrijging informatie op personen (openbare orde)				x		5	3	15	Hoog	Issue: Het is onduidelijk of art. 3 Pw voldoende grondslag biedt voor het verkrijgen van informatie over personen binnen het openbare orde domein. Risico: mogelijk onrechtmatige verkrijging van gegevens.	Neem dit onderdeel mee in het bestaande project waarin de reikwijdte van art. 3 Pw wordt onderzocht.	IB risico	1-1-2024

Privacy	20231214 GEB Wpg_Werven en Beheren Informanten_0.2.docx	Intelligence	Werven en beheren informanten	Uitvoering				x	x	5	3	15	Hoog	Issue: Het gebrek aan uniformiteit in de uitvoering van gegevensverwerking in verschillende politie-eenheden kan leiden tot ongelijke bescherming van privacyrechten voor betrokkenen. Risico: Dit kan resulteren in inconsistenties, onduidelijkheden en mogelijk onjuiste behandeling van persoonlijke gegevens. Betrokkenen kunnen hierdoor verschillende ervaringen hebben met betrekking tot hun privacy, afhankelijk van de eenheid waarmee ze te maken hebben.	Om dit privacyrisico te adresseren, is het belangrijk om uniforme richtlijnen en werkprocessen of procedures op te stellen en deze toe te passen in alle politie-eenheden. Implementeer een uniform beleid voor gegevensverwerking dat geldt voor alle politie-eenheden. Dit beleid moet in overeenstemming zijn met de geldende privacywetgeving en best practices. Het moet duidelijke richtlijnen bevatten over hoe persoonsgegevens moeten worden verzameld, verwerkt, bewaard en gedeeld. Overweeg de mogelijkheid van centraal beheer en coördinatie van gegevensverwerking, waarbij er een duidelijke hiërarchie is voor het toepassen van het beleid. Een centrale autoriteit kan de uniformiteit bewaken en ervoor zorgen dat alle eenheden zich houden aan de vastgestelde normen. Streef naar standaardisatie van systemen en tools die worden gebruikt voor gegevensverwerking. Dit minimaliseert variabiliteit in de implementatie van privacyrichtlijnen.	Werkproces gerelateerd	1-1-2024
Privacy	20231214 GEB Wpg_Werven en Beheren Informanten_0.2.docx	Intelligence	Werven en beheren informanten	Autorisaties					x	5	3	15	Hoog	Issue: Er bestaan geen periodieke controles voor de uitgegeven autorisaties. Risico: 5.1.2.i [redacted]	Implementeer een gestructureerd proces voor het regelmatig (bijvoorbeeld halfjaarlijks of jaarlijks) reviewen en valideren van alle toegekende autorisaties binnen het systeem. Dit proces moet ervoor zorgen dat de huidige autorisaties nog steeds overeenkomen met de taken en verantwoordelijkheden van de betrokken gebruikers. Deze reviews kunnen worden uitgevoerd door systeembeheerders, leidinggevenden of aangewezen autorisatiebeheerders. Implementeer geautomatiseerde tools en systemen voor autorisatiecontroles. Deze tools kunnen regelmatig de autorisaties in het systeem analyseren en afstemmen op de actuele rollen en functies van gebruikers. Bij inconsistenties of onjuiste autorisaties kan het systeem automatisch waarschuwingen genereren voor verdere actie. Dit minimaliseert menselijke fouten en verhoogt de efficiëntie van het autorisatiebeheer.	IB risico	1-1-2024
Privacy	20231214 GEB Wpg_Werven en Beheren Informanten_0.2.docx	Intelligence	Werven en beheren informanten	Verwerkingstermijnen en bewaartermijnen						5	3	15	Hoog	Issue: De daadwerkelijke verwerkingsperiodes van fysiek verwerkte politiegegevens zijn niet transparant en kunnen mogelijk langer zijn dan wettelijk is toegestaan. Hoewel er tijdens het onderzoek geen bewijs is gevonden dat dit plaatsvindt, kan ook niet met zekerheid worden uitgesloten dat het voorkomt. Risico: onrechtmatige gegevensverwerking.	Ontwikkel en implementeer een duidelijk beleid voor gegevensbewaring. Definieer de specifieke periodes gedurende welke bepaalde categorieën gegevens worden bewaard, en zorg ervoor dat deze periodes in overeenstemming zijn met de wettelijke vereisten. Voer regelmatig evaluaties uit van de bewaarde gegevens om te bepalen of ze nog steeds nodig zijn voor het beoogde doel. Als niet, verwijder de gegevens dan conform het retentiebeleid.	Werkproces gerelateerd	1-1-2024
Privacy	20231214 GEB Wpg_Werven en Beheren Informanten_0.2.docx	Intelligence	Werven en beheren informanten	Geen toetsing op 5.1.2.i [redacted] systeem				x	x	5	3	15	Hoog	Issue: De informatiebeveiliger kon en mocht geen toetsing op 5.1.2.i [redacted] -systeem uitvoeren, aangezien dit systeem gevoelige informatie bevat. Risico: Er bestaat een mogelijkheid dat het systeem niet voldoet aan de privacywet- en regelgeving. Dit kan meerdere risico's met zich mee brengen, zoals het verzamelen van meer data dan noodzakelijk is, bewaartermijnen die worden overschreden en autorisaties die niet goed geregeld zijn.	Een mogelijke maatregel om dit privacyrisico te beperken, is het implementeren van strikte autorisatieprotocollen en toegangscontroles voor 5.1.2.i [redacted] -systeem. Dit houdt in dat alleen bevoegde personen met een geldige reden toegang hebben tot de gegevens in het systeem. Daarnaast is het essentieel om het personeel dat toegang heeft tot dergelijke gevoelige systemen adequaat te trainen en bewust te maken van de privacywetgeving en een verantwoordelijke aanwijzen voor het uit voeren van informatie beveiliging analyses.	IB risico	1-1-2024
Privacy	20231214 GEB WPG - Afhandelen Bijzondere Getuige_0.2.docx	Intelligence	Afhandelen bijzondere getuige	Uitvoering				x	x	5	3	15	Hoog	Issue: Het gebrek aan uniformiteit in de uitvoering van gegevensverwerking in verschillende politie-eenheden kan leiden tot ongelijke bescherming van privacyrechten voor betrokkenen. Risico: Dit kan resulteren in inconsistenties, onduidelijkheden en mogelijk onjuiste behandeling van persoonlijke gegevens. Betrokkenen kunnen hierdoor verschillende ervaringen hebben met betrekking tot hun privacy, afhankelijk van de eenheid waarmee ze te maken hebben.	Om dit privacyrisico te adresseren, is het belangrijk om uniforme richtlijnen en werkprocessen of procedures op te stellen en deze toe te passen in alle politie-eenheden. Implementeer een uniform beleid voor gegevensverwerking dat geldt voor alle politie-eenheden. Dit beleid moet in overeenstemming zijn met de geldende privacywetgeving en best practices. Het moet duidelijke richtlijnen bevatten over hoe persoonsgegevens moeten worden verzameld, verwerkt, bewaard en gedeeld. Overweeg de mogelijkheid van centraal beheer en coördinatie van gegevensverwerking, waarbij er een duidelijke hiërarchie is voor het toepassen van het beleid. Een centrale autoriteit kan de uniformiteit bewaken en ervoor zorgen dat alle eenheden zich houden aan de vastgestelde normen. Streef naar standaardisatie van systemen en tools die worden gebruikt voor gegevensverwerking. Dit minimaliseert variabiliteit in de implementatie van privacyrichtlijnen.	Werkproces gerelateerd	1-1-2024

Privacy	20231214 GEB WPG - Afhandelen Bijzondere Getuige_0.2.docx	Intelligence	Afhandelen bijzondere getuige	Autorisaties					x	5	3	15	Hoog	Issue: Er bestaan geen periodieke controles voor de uitgegeven autorisaties. Risico: 5.1.2.i [redacted]	Implementeer een gestructureerd proces voor het regelmatig (bijvoorbeeld halfjaarlijks of jaarlijks) reviewen en valideren van alle toegekende autorisaties binnen het systeem. Dit proces moet ervoor zorgen dat de huidige autorisaties nog steeds overeenkomen met de taken en verantwoordelijkheden van de betrokken gebruikers. Deze reviews kunnen worden uitgevoerd door systeembeheerders, leidinggevenden of aangewezen autorisatiebeheerders. 5.1.2.i [redacted] . Bij inconsistenties of onjuiste autorisaties kan het systeem automatisch waarschuwingen genereren voor verdere actie. Dit minimaliseert menselijke fouten en verhoogt de efficiëntie van het autorisatiebeheer.	IB risico	1-1-2024
Privacy	20231214 GEB WPG - Afhandelen Bijzondere Getuige_0.2.docx	Intelligence	Afhandelen bijzondere getuige	Verwerkingstermijnen en bewaartermijnen						5	3	15	Hoog	Issue: De daadwerkelijke verwerkingsperiodes van fysiek verwerkte politiegegevens zijn niet transparant en kunnen mogelijk langer zijn dan wettelijk is toegestaan. Hoewel er tijdens het onderzoek geen bewijs is gevonden dat dit plaatsvindt, kan ook niet met zekerheid worden uitgesloten dat het voorkomt. Risico: onrechtmatige gegevensverwerking.	Ontwikkel en implementeer een duidelijk beleid voor gegevensbewaring. Definieer de specifieke periodes gedurende welke bepaalde categorieën gegevens worden bewaard, en zorg ervoor dat deze periodes in overeenstemming zijn met de wettelijke vereisten. Voer regelmatig evaluaties uit van de bewaarde gegevens om te bepalen of ze nog steeds nodig zijn voor het beoogde doel. Als niet, verwijder de gegevens dan conform het retentiebeleid.	Werkproces gerelateerd	1-1-2024
Privacy	20231214 GEB WPG - Afhandelen Bijzondere Getuige_0.2.docx	Intelligence	Afhandelen bijzondere getuige	Geen toetsing op 5.1.2.i [redacted] -systeem				x	x	5	3	15	Hoog	Issue: De informatiebeveiliger kon en mocht geen toetsing op 5.1.2.i [redacted] -systeem uitvoeren, aangezien dit systeem gevoelige informatie bevat. Risico: Er bestaat een mogelijkheid dat het systeem niet voldoet aan de privacywet- en regelgeving. Dit kan meerdere risico's met zich mee brengen, zoals het verzamelen van meer data dan noodzakelijk is, bewaartermijnen die worden overschreden en autorisaties die niet goed geregeld zijn.	Een mogelijke maatregel om dit privacyrisico te beperken, is het implementeren van strikte autorisatieprotocollen en toegangscontroles voor 5.1.2.i [redacted] -systeem. Dit houdt in dat alleen bevoegde personen met een geldige reden toegang hebben tot de gegevens in het systeem. Daarnaast is het essentieel om het personeel dat toegang heeft tot dergelijke gevoelige systemen adequaat te trainen en bewust te maken van de privacywetgeving en een verantwoordelijke aanwijzen voor het uit voeren van informatie beveiliging analyses.	IB risico	1-1-2024
Privacy	20231221 GEB Personen met Verward Gedrag_versie 1.0_DEF.pdf	Zorg & Veiligheid	Personen met verward gedrag	Uitvoering						5	3	15	Hoog	Issue: De verwerking wordt in de eenheden niet uniform uitgevoerd. Risico: De verwerking is niet transparant; verwerking is niet beheersbaar als op verschillende locaties verschillende werkwijzen worden gehanteerd.	Onderzoek hoe de landelijke uniformiteit kan worden verbeterd. Bijvoorbeeld door: - Controleer de landelijke werkinstructies op naleving. - Pas waar nodig werkinstructies aan. - Actualiseer het BRM.	Werkproces gerelateerd	1-1-2024
Privacy	20231221 GEB Personen met Verward Gedrag_versie 1.0_DEF.pdf	Zorg & Veiligheid	Personen met verward gedrag	Autorisaties					x	5	3	15	Hoog	Issue: Autorisaties worden niet periodiek gecontroleerd. Risico: Medewerkers kunnen meer gegevens inzien dan noodzakelijk voor de uitoefening van hun taak; datalekken en onrechtmatig gegevensgebruik.	Controleer de autorisaties regelmatig om te voorkomen dat medewerkers meer gegevens inzien dan noodzakelijk is voor de uitoefening van hun taak	IB risico	1-1-2024
Privacy	20231221 GEB Personen met Verward Gedrag_versie 1.0_DEF.pdf	Zorg & Veiligheid	Personen met verward gedrag	Verwerkingstermijnen						5	3	15	Hoog	Issue: Door inzet van e-mail en netwerkschijven is er onvoldoende zicht op of verwerkingstermijnen, waardoor de verwerking mogelijk langer plaatsvindt en de gegevens mogelijk langer toegankelijk zijn dan wettelijk is toegestaan. Risico: o.a. onrechtmatige gegevensverwerking.	Pas systemen en procedures aan om de verwerkingstermijnen na te leven.	IB risico	1-1-2024
Privacy	20231221 GEB Personen met Verward Gedrag_versie 1.0_DEF.pdf	Zorg & Veiligheid	Personen met verward gedrag	Vernietigingstermijnen						1	1	1	Zeer laag	Issue: Formeel gezien wordt niet voldaan aan de vernietigingstermijnen zoals vastgesteld in de Wpg. Risico: o.a. onrechtmatige gegevensverwerking.	Er zijn geen mogelijke maatregelen. De korpschef heeft besloten politiegegevens niet standaard te vernietigen als de bewaartermijn op grond van de Wpg is verstreken in verband met de opsporing van cold cases.	IB risico	1-1-2024
Privacy	20231221 GEB Personen met Verward Gedrag_versie 1.0_DEF.pdf	Zorg & Veiligheid	Personen met verward gedrag	Vernietigingstermijnen						5	3	15	Hoog	Issue: een AOP en een AOL kunnen zichtbaar blijven in BVH, ook als hun geldigheidsduur is verstreken en het niet langer noodzakelijk is kennis te nemen van een AOP of AOL. Risico: o.a. onrechtmatige gegevensverwerking, stigmatisering	Zorg voor een technische aanpassing die ertoe leidt dat AOP's en AOL's na afloop van hun geldigheidsduur niet langer zijn in te zien.	IB risico	1-1-2024
Privacy	20231221 GEB Personen met Verward Gedrag_versie 1.0_DEF.pdf	Zorg & Veiligheid	Personen met verward gedrag	5.1.2.i [redacted]					x	3	5	15	Hoog	Issue: voor de communicatie met ketenpartners over personen met verward gedrag wordt niet consequent gebruik gemaakt van 5.1.2.i [redacted] I of 5.1.2.i [redacted] Risico: o.a. datalekken	Gebruik voor de communicatie met ketenpartners over personen met verward gedrag standaard een beveiligde vorm van communicatie.	IB risico	1-1-2024
Privacy	20231221 GEB Personen met Verward Gedrag_versie 1.0_DEF.pdf	Zorg & Veiligheid	Personen met verward gedrag	Datakwaliteit				x		3	5	15	Hoog	Issue: er worden query's gedraaid op BVH om inzicht te krijgen in incidenten waarbij personen met verward gedrag zijn betrokken, terwijl niet altijd helder is wat de kwaliteit is van de uitkomsten van deze query's en daarop geen toetsing wordt gedaan Risico: onjuistheid van de gegenereerde gegevens	Toets van tijd tot tijd de kwaliteit van de query's en neem maatregelen als deze in te hoge mate onjuiste uitkomsten geven.	IB risico	1-1-2024
Privacy	20231221 GEB Personen met Verward Gedrag_versie 1.0_DEF.pdf	Zorg & Veiligheid	Personen met verward gedrag	Overig						3	5	15	Hoog	Issue: 5.1.2.i [redacted] zijn externe applicaties (dus: politie is hiervan niet de product owner) waarop om die reden vanuit de politie geen IB-analyse kon worden uitgevoerd. Risico: onzeker of deze applicaties voldoende veilig zijn.	Toets bij de externe product owners of de security aspecten van deze applicaties voldoende zijn geregeld en neem indien nodig aanvullende IB-maatregelen	IB risico	1-1-2024
Privacy	20231221 GEB Personen met Verward Gedrag_versie 1.0_DEF.pdf	Zorg & Veiligheid	Personen met verward gedrag	Gegevensverstrekking					x	3	5	15	Hoog	Issue: Binnen deze verwerking vinden veel verstrekkingen plaats. Vanuit het onderzoek en de gesprekken is het beeld ontstaan dat de noodzakelijkheid van de verstrekking niet altijd wordt afgewogen. Er wordt vaak gekozen om de mutaties in zijn geheel te verstrekken i.p.v. alleen de relevante onderdelen. Risico: o.a. onrechtmatige gegevensverstrekking, kans op datalekken.	Instrueer medewerkers om de noodzakelijkheid van de vestrekkingen per casus te beoordelen. Controleer daarnaast periodiek welke gegevens verstrekt worden aan de verschillende ketenpartners.	IB risico	1-1-2024
Privacy	20231221 GEB Personen met Verward Gedrag_versie 1.0_DEF.pdf	Zorg & Veiligheid	Personen met verward gedrag	Gegevensverstrekking			x		x	3	5	15	Hoog	Issue: Op dit moment maakt een politiemedewerker op individuele basis de afweging of en zo ja welke gegevens worden verstrekt, zonder dat hiervoor een uniform en landelijk privacyrechtelijk toetsingskader beschikbaar is. Risico: o.a. onrechtmatige gegevensverstrekking, kans op willekeur, kans op datalekken.	Creëer uniforme en landelijke toetsingskaders vanuit privacyrechtelijk perspectief voor deze verstrekkingen, zodat verstrekkingen uniform en in overeenstemming met de Wpg plaatsvinden. Voer consequent een vierogen principe in bij belangrijke verstrekkingen, zoals bijvoorbeeld bij het doen van een melding aan het meldpunt niet-acuut.	IB risico	1-1-2024

Privacy	20231221 GEB Personen met Verward Gedrag_versie 1.0_DEF.pdf	Zorg & Veiligheid	Personen met verward gedrag	Gegevensverstrekking					x	3	5	15	Hoog	Issue: binnen de kaders van het onderzoek van deze GEB kan niet worden vastgesteld of voor alle verstrekkingen die bedoeld zijn plaats te vinden op basis van artikel 20 Wpg, rechtsgeldige artikel 20 Wpg beslissingen zijn genomen. Risico: o.a. onrechtmatige gegevensverstrekking, kans op datalekken	Recentelijk is een nieuw Beleidskader convenanten met artikel 20 Wpg-beslissingen met bijbehorend(e) checklist, meldingsformulier, instructies dossiervorming, procesbeschrijving en WOO-instructie ter goedkeuring voorgelegd aan de stuurgroep intensivering privacy. Ook zijn convenanten binnen het Programma intensivering privacy gereviewd. Met deze initiatieven krijgt de portefeuille degelijke handvatten om het beheer van de artikel 20 Wpg-beslissingen/convenanten te verbeteren en inzicht te krijgen of de verstrekkingen in samenwerkingsverbanden zijn “gedekt” door rechtsgeldige artikel 20 Wpg beslissingen.	Werkproces gerelateerd	1-1-2024		
Privacy	20231222 Addendum GEB HAVANK4 & CATCH2 dactyloscopie v.1.0 .docx	Specialistische Opsporing	Dactyloscopie	Rechtmatigheid						5	1	5	Midden	De verwerking voor ondersteuning van de politietaak (art. 13 Wpg) heeft geen schriftelijke vastlegging (protocol ex art. 13 lid 1 Wpg) waarin o.a. de frequentie van de controle op de verwerkingstermijnen is vastgelegd.	Beschrijf in een addendum de frequentie waarop de verwerkingstermijnen van de gegevens in de HAVANK-strafrechtdatabase gecontroleerd worden en stel dit vast als onderdeel van het art. 13 protocol.	IB risico	1-1-2024		
Privacy	20231222 Addendum GEB HAVANK4 & CATCH2 dactyloscopie v.1.0 .docx	Specialistische Opsporing	Dactyloscopie	Rechtmatigheid						5	1	5	Midden	De sporen in de HAVANK-strafrechtdatabase worden niet tijdig verwijderd vanwege het ontbreken van de afloopberichten vanuit de strafrechtketen. De betrokkene loopt zo het risico, dat er te veel gegevens worden verwerkt. Ook dreigt hier voor de organisatie een boete en imagoschade.	Treed in overleg met de strafrechtketen om consistent en wellicht geautomatiseerd afloopberichten te verkrijgen.	IB risico	1-1-2024		
Privacy	20231222 Addendum GEB HAVANK4 & CATCH2 dactyloscopie v.1.0 .docx	Specialistische Opsporing	Dactyloscopie	Autorisatie						5	2	10	Hoog	De geautoriseerde bevoegd functionaris (leidend specialist van het Centrum voor Biometrie) is niet als zodanig aangewezen middels een besluit.	Wijs de bevoegd functionaris aan met een besluit.	IB risico	45292		
Privacy	20231222 Addendum GEB HAVANK4 & CATCH2 dactyloscopie v.1.0 .docx	Specialistische Opsporing	Dactyloscopie	Verwerkingstermijnen						5	3	15	Hoog	De verwerkingstermijnen worden niet nageleefd ten aanzien van de dactyloscopische onderzoeksrapporten waardoor de verwerking langer plaatsvindt en de politiegegevens langer toegankelijk zijn dan is toegestaan.	Pas systemen en procedures aan om de verwerkingstermijnen na te leven. Geef de medewerkers de nodige instructies zodat de rapporten tijdig verwijderd worden.	IB risico	45292		
Privacy	231208 GEB Uitvoeren alcohol- en drugstest 1.0.pdf	GGP	Uitvoeren alcohol- en drugstests	Werkproces						4	1	4	Midden	Issue: De verwerking heeft een verouderd werkproces in de bedrijfsarchitectuur. Risico: De verwerking is onvoldoende transparant en beheersbaar. Er staan nu processen in die niet herkenbaar zijn voor de medewerkers.	Zorg dat de werkprocessen geactualiseerd worden in de bedrijfsarchitectuur, centraal vastgesteld zijn en beschikbaar zijn gesteld.	Werkproces gerelateerd	45292	44317	
Privacy	231208 GEB Uitvoeren alcohol- en drugstest 1.0.pdf	GGP	Uitvoeren alcohol- en drugstests	Autorisatie					x	3	4	12	Hoog	Issue: Autorisaties worden niet periodiek gecontroleerd. Risico: De controle op de autorisatie vindt onvoldoende plaats omdat [5.1.2.i] .	Controleer de autorisaties regelmatig [5.1.2.i]	IB risico	45292	44196	
Privacy	231208 GEB Uitvoeren alcohol- en drugstest 1.0.pdf	GGP	Uitvoeren alcohol- en drugstests	Verwerkingstermijnen zijn niet inzichtelijk						5	3	15	Hoog	Issue: Door inzet van [5.1.2.i] is er onvoldoende zicht op of verwerkingstermijnen, waardoor de verwerking mogelijk langer plaatsvindt en de gegevens mogelijk langer toegankelijk zijn dan wettelijk is toegestaan. Risico: o.a. onrechtmatige verwerking, de verwerking is niet beheersbaar en de verwerkingstermijnen kunnen niet worden gewaarborgd.	Pas systemen en procedures aan om de verwerkingstermijnen na te leven. Stuur op juist gebruik middels en voer controles in op [5.1.2.i] om de verwerkingstermijnen na te leven.	IB risico	45292	44317	
Privacy	231208 GEB Uitvoeren alcohol- en drugstest 1.0.pdf	GGP	Uitvoeren alcohol- en drugstests	Bijzondere politiegegevens onvermijdelijk inzichtelijk bij het raadplegen.						4	1	4	Midden	Issue: Er vindt een integrale bevraging plaats van de politiesystemen waarin (bijzondere) politiegegevens voorkomen, hierbij kan gedacht worden aan vergelijkbare antecedenten. Overige bijzondere politiegegevens die voortkomen uit de raadpleging van politiesystemen zijn mogelijk niet aan te merken als onvermijdelijk. Risico: o.a. onrechtmatige gegevensverwerking.	Blijf sturing geven op het juist gebruik van de politiesystemen. Zorg dat medewerkers up to date blijven m.b.t. het wel en niet raadplegen in de politiesystemen. weten wanneer ze wel en niet raadplegen. Om dit privacyrisico te adresseren, is het belangrijk om uniforme richtlijnen en werkprocessen of procedures op te stellen en deze toe te passen in alle politie-eenheden. Implementeer een uniform beleid voor persoonsgegevensverwerking dat geldt voor alle politie-eenheden. Dit beleid moet in overeenstemming zijn met de geldende privacywetgeving en best practices. Het moet duidelijke richtlijnen bevatten over hoe politiegegevens moeten worden verzameld, verwerkt, bewaard en gedeeld. Overweeg de mogelijkheid van centraal beheer en coördinatie van persoonsgegevensverwerking, waarbij er een duidelijke hiërarchie is voor het toepassen van het beleid. Een centrale autoriteit kan de uniformiteit bewaken en ervoor zorgen dat alle eenheden zich houden aan de vastgestelde normen. Streef naar standaardisatie van systemen en tools die worden gebruikt voor persoonsgegevensverwerking. Dit minimaliseert variabiliteit in de implementatie van privacyrichtlijnen. Implementeer een gestructureerd proces voor het regelmatig (bijvoorbeeld halfjaarlijks of jaarlijks) reviewen en valideren van alle toegekende autorisaties binnen het systeem. Dit proces moet ervoor zorgen dat de huidige autorisaties nog steeds overeenkomen met de taken en verantwoordelijkheden van de betrokken gebruikers. Deze reviews kunnen worden uitgevoerd door systeembeheerders, leidinggevenden of aangewezen autorisatiebeheerders. Implementeer tools en systemen voor autorisatiecontroles. Deze tools kunnen regelmatig de autorisaties in het systeem analyseren en afstemmen op de actuele rollen en functies van gebruikers. Bij inconsistenties of onjuiste autorisaties kan het systeem automatisch waarschuwingen genereren voor verdere actie. Dit minimaliseert menselijke fouten en verhoogt de efficiëntie van het autorisatiebeheer.	IB risico	45292	44317	
Privacy	20231221 GEB casescreening versie 1.0.pdf	GGP	Uitvoeren casescreening	Uitvoering				x	x	3	3	9	Midden	Issue: Het gebrek aan uniformiteit in de uitvoering van gegevensverwerking in verschillende politie-eenheden kan leiden tot ongelijke bescherming van privacyrechten voor betrokkenen. Risico: Dit kan resulteren in inconsistenties, onduidelijkheden en mogelijk onjuiste behandeling van politiegegevens. Betrokkenen kunnen hierdoor verschillende ervaringen hebben met betrekking tot hun privacy, afhankelijk van de eenheid waarmee ze te maken hebben.		Werkproces gerelateerd	45292	44196	
Privacy	20231221 GEB casescreening versie 1.0.pdf	GGP	Uitvoeren casescreening	Autorisaties					x	5	3	15	Hoog	Issue: Er bestaan geen periodieke controles voor de uitgegeven autorisaties Risico: [5.1.2.i]		IB risico	45292	44317	
Privacy	20231221 GEB casescreening versie 1.0.pdf	GGP	Uitvoeren casescreening	Verwerkingstermijnen						3	3	9	Midden	Issue: Onvoldoende zicht op of verwerkingstermijnen bij inzet e-mail en netwerkschrijven. Risico: o.a. onrechtmatige gegevensverwerking	Instrueer medewerkers en draag zorg voor privacy awareness.	IB risico	45292	44317	
Privacy	20231221 GEB casescreening versie 1.0.pdf	GGP	Uitvoeren casescreening	Bijzondere politiegegevens						3	3	9	Midden	Issue: Er ontbreken concrete werkinstructies over de omgang met bijzondere politiegegevens in het kader van deze verwerking. Risico: onrechtmatige verwerking	Stel heldere werkinstructies op en instrueer de collega’s	Werkproces gerelateerd	45292	44196	
Privacy	20231221 GEB casescreening versie 1.0.pdf	GGP	Uitvoeren casescreening	Verwerkingstermijnen en bewaartermijnen zijn niet inzichtelijk				x		5	3	15	Hoog	Issue: Verwerkingstermijnen en bewaartermijnen zijn bij gebruik van e-mail, MS-Access en netwerkschijven onvoldoende inzichtelijk en daardoor niet beheersbaar. Risico: o.a. onrechtmatige verwerking, de verwerking is niet beheersbaar en bewaartermijnen kunnen niet worden gewaarborgd.	Stuur op juist gebruik van, en voer controles in op, netwerkschijven om de verwerkingstermijnen en bewaartermijnen na te leven.	IB risico	45292		
Privacy	20231221 GEB casescreening versie 1.0.pdf	GGP	Uitvoeren casescreening	[5.1.2.i]					x	5	3	15	Hoog	Issue: [5.1.2.i] Risico: [5.1.2.i]	[5.1.2.i]	IB risico	45292	44196	
Privacy	20231221 GEB casescreening versie 1.0.pdf	GGP	Uitvoeren casescreening	Gegevensverstrekking						5	3	15	Hoog	Issue: Gegevensverstrekking gebeurt via een geautomatiseerd proces. Risico: Mogelijk onrechtmatige verstrekking doordat er onvoldoende controle bestaat op de politiegegevens die verstrekt worden aan ketenpartners.	Controleer regelmatig of de verstrekkingen juist en rechtmatig worden uitgevoerd.	IB risico	45292	44196	

Privacy	20240222 GEB Uitvoeren digitaal onderzoek_JR.docx	Specialistische Opsporing	Uitvoeren digitaal onderzoek	Bewaar- en vernietigingstermijnen					x	5	4	20	Zeer hoog	Issue: Een onderzoeksdossier wordt door de opsporingsambtenaar van politie in de praktijk pas op afgehandeld gezet na een afdoeningsbericht van het OM. Doordat dit proces niet is geautomatiseerd en/of een afdoeningsbericht structureel achterwege blijft, komt het in de praktijk veelvuldig voor dat dossiers met daarin politiegegevens blijven staan op status “verwerken” en daardoor gegevens langer worden verwerkt dan wettelijk is toegestaan. Risico: Politiegegevens worden langer verwerkt dan de wettelijke termijnen waardoor er langer dan is toegestaan inbreuk wordt gemaakt op de privacy van betrokkenen. Hierdoor kan er imagoschade optreden of kan de politie een last onder bestuursdwang of bestuurlijke boete opgelegd krijgen van de Autoriteit Persoonsgegevens (AP) en andere onderzoeken die starten met deze gegevens een onrechtmatig basis hebben.	Inventariseer in hoeverre wordt voldaan aan de wettelijke bewaar- en vernietigings-termijnen en pak de geconsta-teerde afwijkingen op. Maak afspraken met het OM over tijdige (bij voorkeur geautoma-tiseerde) kennisgeving met betrekking tot het sluiten van een dossier, zodat de wettelijke bewaar- en vernietigings-termijnen gaan lopen. Richt vervolgens een eigen geautoma-tiseerd proces in met betrekking tot de bewaar- en vernietigings-termijnen.	IB risico	45292	44196
Privacy	20240222 GEB Uitvoeren digitaal onderzoek_JR.docx	Specialistische Opsporing	Uitvoeren digitaal onderzoek	Bewaar- en vernietigingstermijnen					x	5	4	20	Zeer hoog	Issue: Momenteel worden politiegegevens die in het politiesysteem BVH staan niet structureel vernietigd. Risico: Politiegegevens worden langer verwerkt dan de wettelijke termijnen waardoor er sprake is van een onrechtmatige verwerking. Als gevolg hiervan wordt er langer dan is toegestaan inbreuk gemaakt op de privacy van betrokkenen. Hierdoor kan er imagoschade optreden of kan de politie een last onder bestuursdwang of bestuurlijke boete opgelegd krijgen van de Autoriteit Persoonsgegevens (AP). Issue: 5.1.2.i [redacted] .	Op grond van de kamerbrief worden politie-gegevens na het verstrijken van de wettelijke bewaartermijn niet vernietigd. De kamerbrief heeft waarde, maar is geen ‘vrijbrief’ om buiten de wet te gaan en de wettelijke bewaartermijn te overschrijden. Richt een procedure in over hoe er in de praktijk moet worden omgegaan met politie-gegevens die voor cold case onderzoek langer worden bewaard dan de termijn die op grond van de Wpg is bepaald. Bepaal welke gegevens langer dan tien jaar bewaard kunnen worden en vernietig de overige gegevens waarvoor de bewaartermijn is verstreken.	IB risico	45292	44196
Privacy	20240222 GEB Uitvoeren digitaal onderzoek_JR.docx	Specialistische Opsporing	Uitvoeren digitaal onderzoek	Bewaar- en vernietigingstermijnen			x	x	x	4	5	20	Zeer hoog	Risico: Politiegegevens zijn hierdoor onvoldoende beschermd en worden langer verwerkt dan de wettelijke termijnen waardoor er sprake is van een onrechtmatige verwerking. Als gevolg hiervan wordt er langer dan is toegestaan inbreuk gemaakt op de privacy van betrokkenen. Hierdoor kan er imagoschade optreden of kan de politie een last onder bestuursdwang of bestuurlijke boete opgelegd krijgen van de Autoriteit Persoonsgegevens (AP) en andere onderzoeken die starten met deze gegevens een onrechtmatig basis hebben	Vernietig politie-gegevens die in Summ-IT staan waarvan de bewaartermijn is verstreken.	IB risico	45292	44196
Privacy	20240222 GEB Uitvoeren digitaal onderzoek_JR.docx	Specialistische Opsporing	Uitvoeren digitaal onderzoek	Verwerkingsregister			x			4	3	12	Hoog	Issue: Afgesloten Verwerkers-overeenkomsten worden structureel niet in het daarvoor bestemde register 5.1.2.i opgeslagen. Risico: 5.1.2.i [redacted]	Beoordeel per verwerking welke ketenpartners bij de verwerking betrokken zijn. Toets vervolgens of de ketenpartner in de zin van artikel 1 sub i Wpg een verwerker is. Zo ja, kijk of er een verwerkers-overeenkomst is afgesloten. Sluit een verwerkers-overeenkomst af indien dit niet is gebeurd. Sla de ondertekende verwerkers-overeenkomst op onder de juiste verwerking in 5.1.2.i	IB risico	45292	44196
Privacy	20240222 GEB Uitvoeren digitaal onderzoek_JR.docx	Specialistische Opsporing	Uitvoeren digitaal onderzoek	Verwerkers-overeenkomst			x		x	4	3	12	Hoog	Issue: Het is onduidelijk of er verwerkers-overeenkomsten zijn gesloten met partners als 5.1.2.i en 5.1.2.i . De verwerkers-overeenkomsten zijn niet in het verwerkingsregister 5.1.2.i geüpload en het is niet duidelijk waar ze wel zijn opgeslagen. Risico: 5.1.2.i [redacted]	Controleer of een verwerkers-overeenkomst is afgesloten. Sluit een verwerkers-overeenkomst af indien deze ontbreekt. Is er wel een verwerkers-overeenkomst, controleer of deze actueel is. Sla de verwerkers-overeenkomst op in 5.1.2.i	IB risico	45292	44196
Privacy	20231130 WPG GEB Problematische Jeugd V.0.25 .docx	Zorg & Veiligheid	Problematische Jeugd	Rechtmatigheid						4	4	16	Hoog	5.1.2.i [redacted]	Beschrijf de verwerking voor de ondersteuning van de politietaak om de verwerking meer te reguleren. Dit dient voorafgaand aan de start van een verwerking plaats te vinden.	IB risico		NVT
Privacy	20231130 WPG GEB Problematische Jeugd V.0.25 .docx	Zorg & Veiligheid	Problematische Jeugd	Werkproces						4	4	16	Hoog	5.1.2.i [redacted] 5.1.2.i [redacted]	5.1.2.i [redacted]	IB risico		NVT
Privacy	20231130 WPG GEB Problematische Jeugd V.0.25 .docx	Zorg & Veiligheid	Problematische Jeugd	Werkproces					x	4	3	12	Hoog	5.1.2.i [redacted]	Leidt medewerkers op in het correct gebruik van de gewezen applicatie, 5.1.2.i of 5.1.2.i .	IB risico		NVT
Privacy	20231130 WPG GEB Problematische Jeugd V.0.25 .docx	Zorg & Veiligheid	Problematische Jeugd	Autorisatie					x	5	3	15	Hoog	5.1.2.i [redacted]	5.1.2.i [redacted] reguliere controle van de autorisaties volgens het beleid of autorisatiematrix.	Werkproces gerelateerd		NVT
Privacy	20231130 WPG GEB Problematische Jeugd V.0.25 .docx	Zorg & Veiligheid	Problematische Jeugd	Autorisatie					x	5	3	15	Hoog	De controle op de autorisatie vindt onvoldoende plaats 5.1.2.i [redacted]	Benoem de systemen waar 5.1.2.i [redacted] moeten plaatsvinden, meld deze bij de FG, vraag aan de productowners wat er voor nodig is om dit gebruikersvriendelijker te maken.	IB risico		NVT
Privacy	20231130 WPG GEB Problematische Jeugd V.0.25 .docx	Zorg & Veiligheid	Problematische Jeugd	Verwerkingstermijnen						5	5	25	Zeer hoog	De verwerkingstermijnen worden niet nageleefd waardoor de verwerking langer plaatsvindt en de gegevens langer toegankelijk zijn dan is toegestaan.	Pas systemen en procedures aan om de verwerkingstermijnen na te leven. Geef de medewerkers de nodige instructies.	IB risico		NVT
Privacy	20231130 WPG GEB Problematische Jeugd V.0.25 .docx	Zorg & Veiligheid	Problematische Jeugd	Doel applicatie					x	5	2	10	Hoog	De verwerking maakt gebruik van 5.1.2.i , een applicatie niet voldoet aan het vigerende beleid.	Maak gebruik van het Portaal Bestandsuitwisseling bij de uitwisseling van bestanden tussen Politie en ketenpartners.	IB risico		NVT
Privacy	20231130 WPG GEB Problematische Jeugd V.0.25 .docx	Zorg & Veiligheid	Problematische Jeugd	Logging & Monitoring		NCSC top-8 item	x	x	x	3	3	9	Midden	5.1.2.i voldoet niet aan de vereisten voor logging, de audittrail van een record kan worden aangepast door de beheerder.	Pas het beleidskader logging en monitoring toe op 5.1.2.i	Werkproces gerelateerd		NVT
Privacy	20231130 WPG GEB Problematische Jeugd V.0.25 .docx	Zorg & Veiligheid	Problematische Jeugd	Grondslag						2	3	6	Midden	De incidentele verstrekking op basis van art. 19 Wpg in die gevallen dat er geen sprake is van een spoedeisend belang voldoet niet aan de wettelijke vereisten die volgen uit de Awb. De betrokkene wordt de gelegenheid ontzegd om zijn zienswijze te geven op de voorgenomen verstrekking.	Geef de betrokkene de gelegenheid om een zienswijze naar voren te brengen of gebruik art. 19 uitsluitend als verstrekkingsgrond in spoedeisende gevallen.	IB risico		Product Owner
Privacy	20231130 WPG GEB Problematische Jeugd V.0.25 .docx	Zorg & Veiligheid	Problematische Jeugd	Grondslag						5	2	10	Hoog	Verstrekkingen worden door individuele politieambtenaren beoordeeld. Dit leidt mogelijk tot verschillen in de verstrekkingen per regio. Ook is er geen landelijk kader dat de verstrekkingen regelt.	Stel een landelijk kader op dat richting geeft aan de verstrekkingen. Onderzoek hoe de landelijke uniformiteit kan worden verbeterd.	IB risico		Product Owner
Privacy	20231121 GEB Wpg-Huiselijk geweld+kindermishandeling versie 1.0.docx	Zorg & Veiligheid	Huiselijk geweld - kindermishandeling	Uitvoering						5	3	15	Hoog	Issue: De verwerking wordt in de eenheden niet uniform uitgevoerd. Risico: De verwerking is niet transparant; verwerking is niet beheersbaar als op verschillende locaties verschillende werkwijzen worden gehanteerd.	Bijvoorbeeld door: - Controleer de landelijke werkinstructies op naleving. - Pas waar nodig werkinstructies aan. - Actualiseer het BRM.	Werkproces gerelateerd		NVT

Privacy	20231121 GEB Wpg-Huiselijk geweld+kindermishandeling versie 1.0.docx	Zorg & Veiligheid	Huiselijk geweld - kindermishandeling	Autorisaties					x	5	3	15	Hoog	Issue: Autorisaties worden niet periodiek gecontroleerd. Risico: Medewerkers kunnen meer gegevens inzien dan noodzakelijk voor de uitoefening van hun taak; datalekken en onrechtmatig gegevensgebruik.	Controleer de autorisaties regelmatig om te voorkomen dat medewerkers meer gegevens inzien dan noodzakelijk is voor de uitoefening van hun taak	IB risico	NVT
Privacy	20231121 GEB Wpg-Huiselijk geweld+kindermishandeling versie 1.0.docx	Zorg & Veiligheid	Huiselijk geweld - kindermishandeling	Verwerkingstermijnen						5	3	15	Hoog	Issue: Door inzet van [redacted] is er onvoldoende zicht op of verwerkingstermijnen, waardoor de verwerking mogelijk langer plaatsvindt en de gegevens mogelijk langer toegankelijk zijn dan wettelijk is toegestaan. Risico: o.a. onrechtmatige gegevensverwerking.	Pas systemen en procedures aan om de verwerkingstermijnen en bewaartermijnen na te leven.	IB risico	NVT
Privacy	20231121 GEB Wpg-Huiselijk geweld+kindermishandeling versie 1.0.docx	Zorg & Veiligheid	Huiselijk geweld - kindermishandeling	Vernietigingstermijnen						1	1	1	Zeer laag	Issue: Formeel gezien voldoen we niet aan de vernietigingstermijnen zoals vastgesteld in de WPG. Risico: o.a. onrechtmatige gegevensverwerking.	Er zijn geen mogelijke maatregelen. De korpschef heeft besloten politiegegevens niet standaard te vernietigen als de bewaartermijn op grond van de Wpg is verstreken in verband met de opsporing van cold cases.	IB risico	NVT
Privacy	20231121 GEB Wpg-Huiselijk geweld+kindermishandeling versie 1.0.docx	Zorg & Veiligheid	Huiselijk geweld - kindermishandeling	[redacted]					x	5	3	15	Hoog	Issue: [redacted] Risico: [redacted]	[redacted]	IB risico	NVT
Privacy	20231121 GEB Wpg-Huiselijk geweld+kindermishandeling versie 1.0.docx	Zorg & Veiligheid	Huiselijk geweld - kindermishandeling	[redacted]						5	3	15	Hoog	Issue: [redacted] Risico: [redacted]	[redacted]	IB risico	NVT
Privacy	20231121 GEB Wpg-Huiselijk geweld+kindermishandeling versie 1.0.docx	Zorg & Veiligheid	Huiselijk geweld - kindermishandeling	Gegevensverstrekking					x	5	3	15	Hoog	Issue: Binnen deze verwerking vinden veel verstrekkingen plaats. Vanuit het onderzoek en de gesprekken is het beeld ontstaan dat de noodzakelijkheid van de verstrekking niet altijd wordt afgewogen. Er wordt vaak gekozen om de mutaties in zijn geheel te verstrekken i.p.v. alleen de relevante onderdelen. Risico: o.a. onrechtmatige gegevensverstrekking, kans op datalekken.	Instrueer medewerkers dat de noodzakelijkheid van de verstrekkingen per casus beoordeeld dient te worden en neem dit waar mogelijk op in werkinstructies. Controleer daarnaast periodiek welke gegevens verstrekt worden aan de verschillende ketenpartners.	Werkproces gerelateerd	NVT