3.

Gegevensbeschermingseffectbeoordeling (PIA)
Zaakonderzoek uitgevoerd met Hansken
Variant 1B "inzet als deskundige"

Ministerie van Justitie en Veiligheid – Nederlands Forensisch Instituut (NFI)

Den Haag, 10 augustus 2020

Vaststelling verwerkersverantwoordelijke: Selecteer/typ datum
Naam: 10.2.e

Advies functionaris voor gegevensbescherming: Selecteer/typ datum
Naam: 10.2.e

Advies CISO:
Naam: 10.2.e

Versiebeheer

Versie	Auteur	Status	Datum	Kern Aanpassingen
0.5	10.2.e	Concept	29 maart 2019	Format aangepast voor Big Data en Nav bespreking
0.6		Concept	11 april 2019	Mn risico paragraaf
0.9		Concept	1 mei 2019	Interne bespreking NFI
0.91		Draft	22 mei 2019	Bespreking met ketenpartners
0.92		Draft 1B	21 aug 2019	Na overleg met OM Politie en doorontwikkeling Hansken
0.93		Draft 1B	23 sept 2019	Variant inzet als 'deskundige in strafzaken'
1.0		Final version	10 aug 2020	Verwerking mgt response

Distributie

Versie	Datum verzending	Naam	Org / Afd	Functie
0.6	11 april 2019	Deelnemers intern overleg NFI	DBS/BV	Specialisten NFI
0.9	1 mei 2019	Deelnemers intern overleg NFI en externe ketenpartners	NFI, OM, Politie, VenJ, FIOD, NVWA, ILenT	Specialisten NFI, externe ketenpartners
0.91	22 mei 2019	Deelnemers intern overleg NFI en externe ketenpartners	NFI, OM, Politie, VenJ, FIOD, NVWA, ILenT	Specialisten NFI, externe ketenpartners
0.93	23 sept 2019	Project- en lijn verantwoordelijken	DBS	
1.0	10 aug 2020			

Gegevensbeschermingseffectbeoordeling (PIA)

Ministerie van Justitie en Veiligheid

Nederlands Forensisch Instituut

Contact:

Laan van Ypenburg 6
2497 GB DEN HAAG
Telefoon (algemeen): (070) 888 66 66

Versie: 1.0

Inhoudsopgave

Inleiding 6

A. Beschrijving kenmerken gegevensverwerkingen 8

1. Voorstel 9
2. Persoonsgegevens 9
3. Gegevensverwerkingen 10
4. Verwerkingsdoeleinden 10
5. Betrokken partijen 11
6. Belangen bij de gegevensverwerking 11
7. Verwerkingslocaties 11
8. Techniek en methode van gegevensverwerking 12
9. Juridisch en beleidsmatig kader 13
10. Bewaartermijnen 14

B. Beoordeling rechtmatigheid gegevensverwerkingen 14

11. Rechtsgrond 14
12. Bijzondere persoonsgegevens 15
13. Doelbinding 16
14. Noodzaak en evenredigheid 16
15. Rechten van de betrokkene 17

C. Beschrijving en beoordeling risico's voor de betrokkenen 19

16. Risico's 19

Algemene risico's 19

Transparantie/rechten betrokkenen 19

Bewaartermijnen 20

Beveiligingsrisico's 20

Toegangs- en autorisatierisico's 20

Beschikbaarheid data 22

Datalek 22

Functionele en kwaliteitsrisico's 23

Meer gegevens dan noodzakelijk 23

Profilering en geautomatiseerde besluitvorming 24

Bewerkings- en/of selectieprogrammatuur is niet betrouwbaar 24

Datakwaliteit/integriteitsrisico's 25

Onrechtmatig datagebruik 26

D. Beschrijving voorgenomen maatregelen 27

17. Maatregelen 27

E. Managementresponse 28

1. Managementreactie DBS op PIA's Hansken (opgesteld door 10.2.e op 3 juli 2020 V1) 28

2. Besprekingsverslag generieke aanbevelingen voor DBS 36

Onderdeel E bevat de managementrespons. Deze bestaat uit 2 delen: ..... **Fout! Bladwijzer niet gedefinieerd.**

- Managementreactie DBS op PIA's Hansken: deze gaat met name in op de Hansken specifieke aspecten; d.d. 3 juli 2020 **Fout! Bladwijzer niet gedefinieerd.**

- Verslag van bespreking met het management van DBS, waarin de generieke aanbevelingen en acties voor digitaal onderzoek voor DBS staan beschreven. D.d. 29 juli 2020 ..... **Fout! Bladwijzer niet gedefinieerd.**

1. Managementreactie DBS op PIA's Hansken ..... **Fout! Bladwijzer niet gedefinieerd.**

Bijlage I Het NFI als verantwoordelijke bij zaakonderzoek door NFI met Hansken in de rol van "deskundige in strafzaken" .. 37

Bijlage II Opbouw en functionaliteit Hansken en Processchema's Hansken 38

Bijlage III Processchema zaakonderzoek met Hansken 39

Bijlage IV Vakbijlage en procesbeschrijving Hansken 40

Bijlage V Memo grondslagen NFI 49

Inleiding

Aanleiding voor de PIA

Deze Privacy Impact Assessment[1] (PIA) heeft betrekking op de verwerkingen van persoonsgegevens die plaatsvinden bij het zaakonderzoek met "Hansken". Hansken is, kort gezegd, de digitale forensische zoekmachine (software/"standaardprogrammatuur" genoemd in de raamovereenkomst) voor forensische zaken die ontwikkeld is door het NFI.

Hansken is ontwikkeld voor het selecteren en ter beschikking stellen van de juiste en relevante (digitale) informatie uit grote bronbestanden in zaken waarnaar (strafrechtelijk) onderzoek gedaan wordt of gedaan moet worden. Dit levert een essentiële en onmisbare bijdrage in het kader van de waarheidsvinding in (straf)zaken.

Daartoe wordt door het NFI een productie-omgeving geboden en diverse andere diensten, die ook vallen onder "Hansken" en die hieronder nader worden toegelicht. "Hansken" is dus een verzamelnaam (software, database en werkomgeving).

Zowel het NFI zelf als de (bijzondere) opsporingsdiensten FIOD, NWVA, IL&T en Politie maken gebruik van Hansken. KMar is tevens voornemens om (diverse onderdelen van) Hansken te gaan gebruiken. Deze partijen kunnen de data in Hansken eenvoudig doorzoeken en uit deze data belangrijk (ontlastend) bewijs halen.

In het kader van "Zaakonderzoek door het NFI met Hansken" worden stelselmatig grote hoeveelheden gewone, bijzondere en strafrechtelijke persoonsgegevens verwerkt. Om deze redenen is het noodzakelijk om een PIA uit te voeren ten aanzien van deze gegevensverwerking. Deze PIA brengt in kaart hoe de verwerking van persoonsgegevens bij het zaakonderzoek met Hansken precies verloopt, wat voor persoonsgegevens er worden verwerkt, welke privacyrisico's hieraan verbonden zijn en hoe deze risico's gemitigeerd (kunnen) worden.

Doel van de PIA

Het doel van deze PIA is:

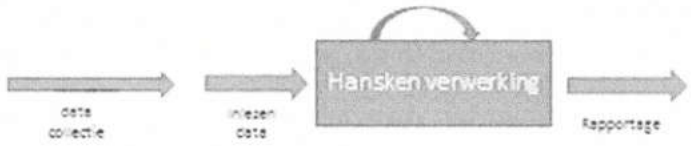
- Het inzichtelijk maken van de verwerking van persoonsgegevens ten behoeve van de kerntaken van het NFI met gebruik van Hansken;
- Het beoordelen van de effecten van de verwerking op de persoonlijke levenssfeer van de betrokkenen (degenen op wie de persoonsgegevens betrekking hebben);
- Het op basis van deze beoordeling waar nodig maatregelen te treffen om deze effecten voor betrokkenen te voorkomen of te verkleinen.

Het doel van Hansken is om de juiste personen, op het juiste moment, toegang te geven tot de juiste informatie. Met Hansken kan een onderzoeksteam snel en efficiënt zoeken in grote hoeveelheden aangeleverde gegevens van dragers, zoals computers en mobiele telefoons. Op alles wat relevant kan zijn, kan worden gezocht, bijvoorbeeld op woorden en namen of eigenschappen van sporen, zoals chatberichten, e-mails of foto's al dan niet gemaakt met een bepaalde camera.
Rechercheurs kunnen met de forensische dienst de zoekresultaten blijven filteren totdat er van die miljoenen sporen een selectie is, waarvan de sporen één op één te bekijken zijn.

Reikwijdte van de PIA

Zaakonderzoek met Hansken kan in verschillende gebruiksvarianten worden uitgevoerd. Zie onderstaand schema:

[1] In het Nederlands wordt dit "Gegevensbeschermingseffectbeoordeling" (GEB) genoemd.



Variant nr	Data collectie	Inlezen door	Onderzoek door	Rapportage door	Host/Housing verantwoordelijke	Technical support	Opmerking
1	Opdrachtgever	NFI	NFI	NFI	NFI	NFI	Object van onderzoek
2	Opdrachtgever	NFI	Opdrachtgever	Opdrachtgever	NFI	NFI	Komt voor bij NVWA en I&T
3	Opdrachtgever	Opdrachtgever	Opdrachtgever	Opdrachtgever	NFI	NFI	Komt niet voor
4	Opdrachtgever	Opdrachtgever *	Opdrachtgever	Opdrachtgever	On Premise	NFI	Komt voor bij politie en FIOD

* Politie laat data soms inlezen door NFI

Deze PIA richt zich op het zaakonderzoek volledig uitgevoerd door het NFI: Variant 1

Binnen variant 1 kan het NFI in twee hoedanigheden acteren.

A. Als onderzoeker in opdracht van het OM, waarbij het OM hoofdzakelijk de interpretatie van de vraagstelling en de uitvoering bepaalt
B. Als 'deskundige in strafzaken', waarbij het NFI volledig zelfstandig en onafhankelijk het zaakonderzoek uitvoert in opdracht van de rechter-commissaris

Zie onderstaand schema.

Verdieping wettelijk kader voor opsporing en bewijsvoering

Nr	Input	Doel	Op-dracht-gever	Wette-lijk regim e	Toelich-ting	Vereist	Rol	Product	Opmer -king
A	Dataset onder titel 3v Regime Wjsg en Wpg (art 9 en 10)	Opsporing	OM die politie de Wpg data laat doorzoeken door NFI	Wpg Wjsg / AVG	Analyse opdracht, die door NFI met Hansken kan worden uitgevoerd	Opdracht DVO en verwer-kersover-eenkomst	Gezamenlijk verwerkings-verantwoor-delijke OM en NFI	Analyse / rapportage	Variant 1
B	Dataset onder titel 3v Regime Wjsg en Wpg	Bewijs-voering Als deskundige (Wet Deskundige Strafzaken)	RC in kader van inzet als deskundige	AVG	NFI treedt op als onafhankelijk instituut en kan hiervoor Hansken inzetten	Opdracht en Aanstelling als deskundig e	Verwerkings-verantwoor-delijke = NFI	Deskundige Rapport	Variant 1
C		Contra expertise	RC		Wordt behandeld als B				Komt voor als B
D	Wjsg en Wpg data	Weten-schappelijk onderzoek	NFI	AVG	Voor ontwikkeling software	Specifieke toestemmi ng	Verwerkings verantwoor-delijke = NFI	Software modules	Buiten scope

Deze PIA richt zich alleen op de hoedanigheid van het NFI optredend als 'deskundige in strafzaken': Variant 1B.

Opmerkingen:

1. De risico's die gepaard gaan met de verwerkingen voor wat betreft de digitale zoekmachine Hansken, zullen vergelijkbaar zijn met de risico's die spelen voor andere 'big data'-verwerkingen binnen het NFI[2].
2. De risico's die in de onderhavige PIA gericht op variant 1B zullen veelal representatief zijn voor de andere verwerkingsvarianten.

A. Beschrijving kenmerken gegevensverwerkingen

Beschrijf op gestructureerde wijze de voorgenomen gegevensverwerkingen, de verwerkingsdoeleinden en de belangen bij de gegevensverwerkingen.

Onder A wordt de eerste stap beschreven van de PIA: een overzicht van de relevante feiten van de voorgenomen gegevensverwerkingen. Als de feiten onduidelijk zijn, werkt dit door in de beoordeling.

[2] In overleg met de Functionaris voor de Gegevensbescherming van JenV is besloten dat het NFI drie grote PIA's zal uitvoeren, die gezamenlijk als dekkend voor het hele NFI zullen worden beschouwd. Dit zijn de PIA's voor Hansken, Promis/BiS en de DNA-databank.

1. Voorstel

Beschrijf het voorstel waar de gegevensbeschermingseffectbeoordeling op ziet en context waarbinnen deze plaatsvindt op hoofdlijnen.

Deze gegevensbeschermingseffectbeoordeling heeft betrekking op het door het NFI uitgevoerd zaakonderzoek met gebruik van Hansken, en waarbij het NFI optreedt als 'deskundige strafzaken' (Wet deskundige in Strafzaken) in opdracht van de Rechter-commissaris (RC). De RC geeft opdracht tot de uitvoering van het onderzoek en benoemt de deskundige om zaakonderzoek uit te voeren en om een deskundige rapport uit te brengen. Het rapport heeft als doel om op de rechtszitting de rechtbank voor te lichten.
Het NFI is in deze gevallen verwerkingsverantwoordelijk en de AVG is het wettelijke regime voor de verwerking van persoonsgegevens (zie bijlage 1).

Dynamiek: Het kan voorkomen dat een zaakonderzoek verandert van aard. Het zaakonderzoek start met doel van opsporing en gaat later over naar een uitvoering in de rol van 'deskundige in strafzaken'. Voor een dergelijke wisseling zal ook een nieuwe aanvraag worden ingediend door de opdrachtgever.

2. Persoonsgegevens

Som alle categorieën van persoonsgegevens op die worden verwerkt. Geef per categorie van persoonsgegevens tevens aan op wie die betrekking hebben. Deel deze persoonsgegevens in onder de typen: gewoon, bijzonder, strafrechtelijk en wettelijk identificerend.

Met Hansken kunnen alle categorieën persoonsgegevens verwerkt worden, omdat deze opgenomen zijn in SVO's (stukken van overtuiging). Het gaat in Hansken meestal om inbeslaggenomen en/of gevorderde data (pc's, servers, mobiele telefoons, fotocamera's, etc.). Bijvoorbeeld: informatie uit een mobiele telefoon bevat o.a. foto's, namen, telefoonnummers, e-mails, metadata, locatiegegevens, betaalgegevens, video's, gegevens over religieuze opvattingen of gezondheid etc. Het kan dus gaan om gewone, gevoelige of bijzondere persoonsgegevens. Hansken kan ook gebruikt worden voor het verwerken van strafrechtelijke gegevens.

Op wie hebben de gegevens betrekking
Het betreft meestal gegevens van veel meer personen dan alleen degene(n) op wie het onderzoek zich richt. Er kunnen dus ook persoonsgegevens verwerkt worden van personen, die niets met de zaak te maken hebben, maar alleen tot de kennissenkring of de interessesfeer van het subject behoren. Er kunnen dus meer betrokkenen[3] zijn dan de verdachten. Het is niet mogelijk vooraf vast te stellen welke van deze persoonsgegevens voor de uitkomst van het onderzoek uiteindelijk wel en niet noodzakelijk zijn en het is ook niet mogelijk om het onderzoek uit te voeren zonder de persoonsgegevens van de 'overige' betrokkenen. Dus de belangrijkste oorzaak van de mogelijke verwerking van teveel betrokkenen is dat vooraf de rol van de overige betrokkenen niet bekend is. En de potentiele verwijdering van bijvoorbeeld een toevallige contactpersoon in de data vergt een onevenredige grote inspanning. In die zin kan dus niet voldaan worden aan 'dataminimalisatie'.

Categorieën betrokkenen
Er kan geen uitputtende lijst gemaakt worden van de categorieën van betrokkenen van wie persoonsgegevens worden verwerkt en verzameld in Hansken. Juist omdat er zo'n grote hoeveelheid aan data wordt verwerkt, kan niet op voorhand vastgelegd worden van welke betrokkenen data in Hansken zit. Het kan hier, gaan om:

- veroordeelde(n)
- verdachte(n)
- slachtoffer(s)
- getuige(en)
- derden die niets met het (strafrechtelijk)onderzoek te maken hebben, of personen die ten onrechte verdacht worden.

Daarnaast worden, om de aanvraag in uitvoering te kunnen nemen, persoonsgegevens verwerkt van de volgende betrokkenen in de Hansken autorisatie module:

- Functionarissen van het NFI/team Hansken;
- Functionarissen en contactpersonen van instanties die producten of diensten of diensten van het NFI afnemen, zijnde de ketenpartners OM, politie, NVWA, IL&T en FIOD.

3. Gegevensverwerkingen

Geef alle voorgenomen gegevensverwerkingen weer.

In bijlage III is de opbouw en functionaliteit van Hansken weergegeven, met daarop aansluitend het processchema dat weergeeft hoe de gegevensverwerking verloopt.
In bijlage IV staat een uitgebreide beschrijving van dit zaakonderzoek met Hansken.

4. Verwerkingsdoeleinden

Beschrijf de doeleinden van de voorgenomen gegevensverwerkingen.

[3] Een betrokkene is voor de AVG degene wiens persoonsgegevens worden verwerkt.

Hansken is, aansluitend op de beschrijving van verwerkingen/producten de digitale zoekmachine (software/"standaardprogrammatuur" genoemd in de raamovereenkomst) voor forensisch onderzoek.

Hansken is ontwikkeld voor het selecteren en ter beschikking stellen van de juiste en relevante (digitale) informatie uit grote bronbestanden in zaken waarnaar (strafrechtelijk) onderzoek gedaan wordt of gedaan moet worden.

Het bieden van software, servers en diensten die daarbij ondersteunend zijn, alsmede de verwerking van persoonsgegevens met behulp van die software en servers, die bijdragen aan het in stand houden en verder ontwikkelen van een digitale zoekmachine ten behoeve van forensisch zaakonderzoek.

1.

5. Betrokken partijen

Benoem welke organisaties betrokken zijn bij welke gegevensverwerkingen. Deel deze organisaties per gegevensverwerking in onder de rollen: verwerkingsverantwoordelijke, verwerker, verstrekker en ontvanger. Benoem tevens welke functionarissen binnen deze organisaties toegang krijgen tot welke persoonsgegevens.

Zoals genoemd treedt het NFI op als verwerkingsverantwoordelijke. Zie hierover tevens bijlage I: "Het NFI als verantwoordelijke".

Afnemers[4]
De *mogelijke* afnemers van persoonsgegevens die in het kader van Hansken zijn verwerkt, zijn (gerelateerd aan de doelstellingen van de verwerking). Binnen de scope van deze PIA is de RC de afnemer van het deskundige rapport.

6. Belangen bij de gegevensverwerking

Beschrijf alle belangen die de verwerkingsverantwoordelijke en anderen hebben bij de voorgenomen gegevensverwerkingen.

Belangen van de gegevensverwerking:

Alle betrokken partijen hebben als belang bij de gegevensverwerking de (ondersteuning van) de waarheidsvinding in strafzaken, en daartoe:

- Indexeren van SVO's en andere stukken/data; en/of
- Het analyseren van grootschalige databestanden
- En uit deze data belangrijk (ontlastend) bewijs halen.
-

Dit is nodig omdat het zeer tijdrovende bezigheden zijn om deze bestanden te doorzoeken en de opsporingscapaciteit schaars is.

7. Verwerkingslocaties

Benoem in welke landen de voorgenomen gegevensverwerkingen plaatsvinden.

[4] Het PIA-format van JenV spreekt over "ontvangers", echter in de Regeling taken NFI wordt gesproken over "afnemers", dus deze laatste term wordt aangehouden.

Nederland (Apeldoorn)

8. Techniek en methode van gegevensverwerking

Beschrijf op welke wijze en met gebruikmaking van welke (technische) middelen en methoden de persoonsgegevens worden verwerkt. Benoem of sprake is van (semi-)geautomatiseerde besluitvorming, profilering of big data-verwerkingen en, zo ja, beschrijf waaruit een en ander bestaat.

(Semi-)geautomatiseerde besluitvorming
Aan de hand van de gegevens die in zaakonderzoek met Hansken-software worden verwerkt , worden geen (semi-)geautomatiseerde besluiten genomen die voor de betrokkenen rechtsgevolgen hebben of hem anderszins in aanmerkelijke mate treffen. Het selectie- en analyseproces met behulp van de Hansken start aan de hand van de zoekcriteria van de onderzoeker. In de loop van het analyseproces voegen medewerkers labels en notities toe die het zoekproces verder richting geven en deze worden bewaard als apart onderdeel van de data. Uiteindelijke besluiten ten aanzien van betrokkenen op grond van de gegevens uit Hansken worden altijd genomen door personen (bijvoorbeeld de Officier van Justitie of de rechter) en zijn dus niet (volledig) geautomatiseerd. Voorafgaand aan de analyse detecteert de analysesoftware tekstblokken, die niet betrokken mogen worden in het onderzoek omdat ze betrekking hebben op geheimhouders (bijvoorbeeld overleg van de verdachte met zijn advocaat of overleg met een medicus over zijn eigen gezondheid). Selectie gebeurt op basis van vooraf gedefinieerde zoektermen. De uitgesloten tekstdelen worden achteraf beoordeeld door een medewerker met specifieke autorisaties.

Profilering
Hansken kan gebruikt worden voor profilering; echter dan vindt dit plaats op initiatief van onderzoekers (net als bij een handmatige verwerking; Hansken als applicatie profileert de data niet). Aan de hand van bepaalde gegevens worden dan namelijk persoonlijke aspecten van natuurlijke personen geëvalueerd, zoals locatie, gedrag, etc. Zo kan bijvoorbeeld aan de hand van SVO's en bewijsstukken die met elkaar gecombineerd worden de locatie of (strafbaar)gedrag van een verdachte worden vastgesteld. Uiteindelijk wordt hierover altijd een besluit genomen door menselijke tussenkomst (bijvoorbeeld de onderzoeker of de rechter).

Algoritmen
Algoritmen en methoden die bij data-analyses worden gebruikt, moeten verder deugdelijk zijn en aan de wetenschappelijke criteria voor goed (statistisch) onderzoek voldoen. Bij voorkeur worden algoritmen gebruikt die wetenschappelijk zijn getoetst, blijkend uit bijvoorbeeld publicaties of peer reviews. Voorbeelden hiervan zijn het gebruik van de National Software Reference Library, waar Hansken een kenmerk "van dit stukje data is bekend dat het onderdeel is van een bekend stuk software en daarmee typisch niet interessant voor onderzoek" overneemt en deze markeert op een forensische spoor. Hierbij wordt gebruik gemaakt van NIST standaards. Een ander voorbeeld is het geautomatiseerd herkennen van inhoud van beeldmateriaal, waarbij Hansken internationaal en wetenschappelijk gevalideerde technieken gebruikt om een foto bijvoorbeeld kenmerk "hier staat mogelijk een wapen op" geeft. De algoritmen worden niet vrijgegeven omdat dit mogelijk het opsporingsproces zou kunnen schaden. Wel wordt inzage gegeven aan de verdediging over hoe de data in een bepaalde zaak zijn verwerkt. Na toestemming van de Rechter Commissaris kan inzage worden gegeven in welke zoekvragen gesteld zijn in Hansken en welke delen van de data gebruikt zijn om de tenlastelegging te ondersteunen. In bijzondere gevallen kunnen zogenaamde datarooms ter beschikking worden gesteld aan de advocatuur. Dit zijn tijdelijke extra omgevingen die worden opgezet om de advocatuur inzicht te geven in een enkele zaak

Big data
Hansken maakt gebruik van big data: door het gebruik van grote hoeveelheden gestructureerde en ongestructureerde data uit verschillende bronnen wordt er data geanalyseerd, waarbij naar gegevens en correlaties wordt gezocht die kennis kunnen opleveren om te kunnen toepassen voor beslissingen. Er worden grote hoeveelheden data geanalyseerd om aan de hand daarvan kennis te vergaren over bijvoorbeeld een verdachte.

9. Juridisch en beleidsmatig kader

Benoem de wet- en regelgeving, met uitzondering van de AVG en de Richtlijn, en het beleid met mogelijke gevolgen voor de gegevensverwerkingen.

- De Regeling taken NFI: bijzondere persoonsgegevens in samenhang met de SLA[5]. Zie voor de specifieke onderdelen van de regeling taken per verwerking paragraaf A1.
- De Wet Deskundige in Strafzaken /DIS (bijzondere persoonsgegevens in samenhang met de SLA).
- Overige bepalingen van het Wetboek van Strafvordering die relevant zijn voor (de onderzoekers van) het NFI.
- Verdragen, zoals het Verdrag van Prüm en Internationale Rechtshulpverdragen, voor zover relevant in een bepaald zaakonderzoek.

10. Bewaartermijnen

Bepaal en motiveer de bewaartermijnen van de persoonsgegevens aan de hand van de verwerkingsdoeleinden.

Er zijn vooralsnog geen bewaartermijnen vastgesteld voor de gegevens die met Hansken verwerkt worden. De bewaartermijnen voor het NFI zullen nader bepaald moeten worden. Wat betreft bewaartermijnen zullen er NFI-breed beslissingen moeten worden genomen en geïmplementeerd. Onderdeel hiervan is mogelijk de aanbeveling om de bewaartermijnen van de politie (vijf jaar) te gaan volgen voor onderzoeken waarvoor dit niet specifiek omschreven is in de wet.

B. Beoordeling rechtmatigheid gegevensverwerkingen

Beoordeel aan de hand van de feiten zoals vastgesteld in onderdeel A of de voorgenomen gegevensverwerkingen rechtmatig zijn. Het gaat hier om de beoordeling van de juridische rechtsgrond, noodzaak en doelbinding van de gegevensverwerkingen. Beoordeel tevens de wijze waarop invulling wordt gegeven aan de rechten van de betrokkenen. Voor dit onderdeel van de PIA is in het bijzonder juridische expertise nodig.

11. Rechtsgrond

Bepaal op welke rechtsgronden de gegevensverwerkingen worden gebaseerd.

[5] Zie ook bijlage V: "Grondslagen voor primaire verwerkingen van persoonsgegevens van het Nederlands Forensisch Instituut".

De grondslagen voor het verwerken van gewone gegevens zijn:

1. De verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang;
2. De verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting.

(artikel 6, lid 1, sub c en d, AVG).

De Regeling taken NFI is een specifieke wettelijke uitwerking van een taak van algemeen belang. De specifieke artikelen uit de regeling taken die van toepassing zijn op (de verschillende onderdelen van) Hansken, zijn :

1. Zaakonderzoek: kerntaak 1 (K1) van het NFI (artikel 1, lid 1 sub a), zoals bedoeld in de Regeling Taken "het verrichten van onafhankelijk forensisch zaakonderzoek op overwegend technisch, medisch-biologisch en natuurwetenschappelijk gebied en het ter zake daarvan uitbrengen van verslag"[6].
2. Inladen van persoonsgegevens: artikel 1, lid 2, sub a uit de Regeling Taken NFI: "een activiteit die in het verlengde ligt van de kerntaken en een onlosmakelijke samenhang heeft met de waarheidsvinding in strafzaken".
3. Technische ondersteuning: artikel 1, lid 2, sub a uit de Regeling Taken NFI: "een activiteit die in het verlengde ligt van de kerntaken en een onlosmakelijke samenhang heeft met de waarheidsvinding in strafzaken".
4. Ontwikkelen van software: kerntaak 2 (K2) uit de Regeling Taken (artikel 1, lid 1, sub b): "het ontwikkelen en implementeren van nieuwe onderzoeksmethoden en technieken ter bevordering van kennis op het gebied van forensisch onderzoek".
5. (Zaakonderzoek politie en FIOD: niet van toepassing voor NFI.)
6. Cursussen/trainingen gebruik Hansken: kerntaak 3 (K3) uit de Regeling Taken (artikel 1, lid 1, sub c): "het zijn van (inter)nationaal kennis- en expertisecentrum op het gebied van forensisch onderzoek".

De verplichting voor het NFI om persoonsgegevens te verwerken kan in een voorkomend geval voortvloeien uit de Wet Deskundigen in strafzaken (Wet DIS). Deskundigen van het NFI kunnen op grond van deze wet van de rechter-commissaris opdrachten krijgen voor het uitvoeren van een deskundigenonderzoek.

Voor meer informatie wat betreft de grondslag voor de verwerking van gewone persoonsgegevens wordt verwezen naar de 'notitie grondslagen' in bijlage V.

Verder heeft de rechter in de uitspraak in de Ennetcom-zaak (ECLI:NL:RBAMS:2018:2504) geoordeeld dat de resultaten uit Hansken verkregen niet onbetrouwbaar zijn, de werkwijze door de verdediging in voldoende mate te controleren zijn geweest en dat voor de inzet van dergelijke hulpmiddelen geen specifieke wettelijke grondslag (zoals voor technische hulpmiddelen o.g.v. in de zin van art. 126ee Sv) vereist is.

12. Bijzondere persoonsgegevens

Indien bijzondere of strafrechtelijke persoonsgegevens worden verwerkt, beoordeel of één van de wettelijke uitzonderingen op het verwerkingsverbod van toepassing is. Bij verwerking van een wettelijk identificatienummer beoordeel of dat is toegestaan.

[6] Art. 1, lid 1, sub a van de Regeling van de Minister van Veiligheid en Justitie, d.d. 8 mei 2012, nr. 2277743, houdende bepalingen inzake de taakopdracht van het Nederlands Forensisch Instituut (Regeling taken NFI).

De verwerking van bijzondere persoonsgegevens binnen het NFI en in het bijzonder in de Hansken omgeving is noodzakelijk om redenen van algemeen belang, op grond van het Unierecht of Nederlands recht (art. 9 lid 2 onder g AVG). Het NFI voldoet tevens aan de volgende vereisten die aan deze grondslag worden gesteld:

- Het waarborgen van de evenredigheid met het nagestreefde doel wordt gewaarborgd *(zie voor meer informatie punt 14 van deze PIA)*
- Wezenlijke eerbiediging van de inhoud van het recht op bescherming van persoonsgegevens
- Er worden passende en specifieke maatregelen genomen ter bescherming van de grondrechten en de fundamentele belangen van betrokkenen *(zie voor meer informatie de over risico's en risicobeperkende maatregelen in punt 16 van deze PIA).*

Hier is de samenloop met o.a. de Regeling taken van het NFI (zie hiervoor) in samenhang met de SLA van belang.

Voor wat betreft de strafrechtelijke persoonsgegevens in Hansken kan het NFI zich beroepen op de volgende uitzondering in art. 10 AVG: "het verwerken onder toezicht van de overheid of indien de verwerking is toegestaan bij Unierechtelijke of lidstaatrechtelijke bepalingen die passende waarborgen voor de rechten en vrijheden van de betrokkenen bieden."

Ook hier is de samenloop met o.a. de Regeling taken van het NFI in samenloop met de SLA van belang.

Voor meer informatie wordt verwezen naar de 'notitie grondslagen' in bijlage V.

13. Doelbinding

Indien de persoonsgegevens voor een ander doel worden verwerkt dan oorspronkelijk verzameld, beoordeel of deze verdere verwerking verenigbaar is met het doel waarvoor de persoonsgegevens oorspronkelijk zijn verzameld.

De persoonsgegevens worden niet voor een ander doel verwerkt dan waarvoor ze zijn verzameld, namelijk voor de uitvoering van het zaakonderzoek. Persoonsgegevens van een specifieke zaak, worden niet gecombineerd met persoonsgegevens uit een andere zaak, tenzij de RC daar aan het NFI specifiek opdracht voor heeft gegeven.

14. Noodzaak en evenredigheid

Beoordeel of de voorgenomen gegevensverwerkingen noodzakelijk zijn voor het verwezenlijken van de verwerkingsdoeleinden. Ga hierbij in ieder geval in op proportionaliteit en subsidiariteit.

a. **Proportionaliteit: staat de inbreuk op de persoonlijke levenssfeer en de bescherming van de persoonsgegevens van de betrokkenen in evenredige verhouding tot de verwerkingsdoeleinden?**
b. **Subsidiariteit: kunnen de verwerkingsdoeleinden in redelijkheid niet op een andere, voor de betrokkene minder nadelige wijze, worden verwezenlijkt?.**

De toets op proportionaliteit en subsidiariteit zal veelal bij de opdrachtgever liggen en in mindere mate bij het NFI.

Proportionaliteit
Het toegang hebben en kunnen analyseren van een grote hoeveelheid gegevens is cruciaal in het proces van waarheidsvinding. Zonder Hansken zijn dergelijke grote databestanden niet binnen redelijke termijn doorzoekbaar. Daarom kan geoordeeld worden dat het middel in verhouding staat tot het doel dat wordt nagestreefd.

Subsidiariteit
Gezien de grote hoeveelheid data die onderzocht kan en moet worden in het kader van waarheidsvinding is er geen minder ingrijpende manier dan met behulp van de Hansken-software en ondersteuning. Verder kan het doel niet bereikt worden, wanneer er minder gegevens verwerkt zouden worden in Hansken. Voor de waarheidsvinding in (straf)zaken is het namelijk van groot belang dat er niet te *weinig* gegevens verzameld worden, omdat er juist zo'n volledig mogelijk beeld gecreëerd moet worden van een situatie/verdachte, overigens ook ter ontlasting van de verdachte. Een relevante onderzoeksvraag kan bijvoorbeeld zijn: "Komt X in het bestand voor?" Een dergelijke vraag kan alleen beantwoord worden door al het beschikbare materiaal te doorzoeken. Alle gegevens die in Hansken verwerkt worden zijn noodzakelijk voor het bereiken van het doel, juist omdat er gezocht wordt naar schakels in een proces die kunnen dienen als bewijsmateriaal. Van te voren is niet altijd vast te stellen om welke/wat voor soort gegevens en om welke betrokkenen het gaat.

15. Rechten van de betrokkene

Geef aan hoe invulling wordt gegeven aan de rechten van betrokkenen. Indien de rechten van de betrokkene worden beperkt, bepaal op grond van welke wettelijke uitzonderingen dat is toegestaan.

Het NFI hanteert een specifiek opgestelde procedure voor de rechten van betrokkenen, op basis van de relevante bepalingen uit de AVG. Het tegemoetkomen aan de rechten van betrokkenen is voor het NFI, in het bijzonder voor de verwerkingen die met behulp van Hansken plaatsvinden, niet altijd mogelijk. De kans bestaat dat in bepaalde gevallen de waarheidsvinding, rechtsgang of strafzaak belemmerd of gefrustreerd wordt wanneer er toegekomen wordt aan de rechten van betrokkenen. In dergelijke gevallen zal het NFI dan ook niet tegenmoetkomen aan verzoeken. Dit wordt hieronder nader toegelicht.

Bij de informatieverplichting en de rechten van betrokkenen voor wat betreft de kerntaken van het NFI zijn de volgende aspecten voor de afhandeling van belang.

1. Bij het verwerken van persoonsgegevens ten behoeve van de uitvoering van de werkzaamheden m.b.t. Hansken, op basis van de kerntaken van het NFI, verkrijgt de NFI opdrachten / verzoeken van de rechter (commissaris), het openbaar ministerie, de nationale politie, en de bijzondere opsporingsdiensten.
2. Het bijzondere hiervan is, dat er samenloop ontstaat met tussen de regimes van de AVG, de UAVG, de Richtlijn Opsporing en Vervolging (uitgewerkt in de Wet Strafvorderlijke en justitiële gegevens en de Wet politiegegevens) en het Wetboek van Strafvordering. [7]
3. Het NFI heeft in voorkomende gevallen een geheimhoudingverplichting ingevolge het Wetboek van Strafvordering (Wet Deskundigen in strafzaken) in het belang van de opsporing en vervolging. Dit geldt ook voor de persoonsgegevens / opdrachten / verzoeken op basis van Wet Strafvorderlijke en justitiële gegevens en de Wet politiegegevens.
4. De informatieplicht in de Wet Strafvorderlijke en justitiële gegevens en de Wet politiegegevens is ondergeschikt aan die in het Wetboek van strafvordering, hetgeen betekent, dat een verdachte over de opdracht aan het NFI door de rechter commissaris en het openbaar ministerie langs strafvorderlijke weg wordt geïnformeerd. Evenzeer aan de geheimhoudingsverplichting ingevolge de Wet Strafvorderlijke en justitiële gegevens en de Wet politiegegevens.
5. Aan de informatieplicht jegens betrokkenen wordt door de politie en het openbaar ministerie uitvoering gegeven door middel van het verstrekken van informatie via hun websites. Het NFI sluit hierbij met zijn website aan. De privacystatement van het NFI zou hiervoor echter wel nader uitgewerkt en gelaagd moeten worden.
6. Ingeval van een informatieverplichting en een verzoek inzake de rechten van betrokkenen op grond van de AVG zal het NFI altijd met het bovenstaande rekening moeten houden.
7. Veelal zal dit betekenen, dat het NFI voor wat betreft de informatieverplichting en verplichtingen aangaande de rechten van betrokkenen een beroep zal doen op de uitzonderingsgronden in de UAVG, met name artikel 41, lid 1, sub d UAVG.
8. Ingeval van een verzoek inzake rechten van betrokkenen, zal het NFI, afhankelijk van de aard van het verzoek, zo nodig over de afhandeling ervan eerst overleggen met de betreffende opdrachtgever. In het afhandelingsbericht aan verzoeker dient er rekening mee te worden gehouden, dat ook een kennisgeving van een doorverwijzing naar een opdrachtgever het opsporings- en vervolgingsproces kan belemmeren of schade toe brengen.

---

[7] Dit is onder meer het geval bij:

a. een opdracht van de rechter, de RC, het openbaar ministerie en politie aan het NFI op grond van het Wetboek van Strafvordering (o.a. de artikelen 51i t/m 51m; 150 t/m 151i WvSv; 227 t/m 237;)
b. de doorwerking van overweging 39, art. 12 t/m 13 Richtlijn Opsporing en Vervolging in art. 24a en 24b Wpg en art. 39 ha Wjsg (publicatie informatie over de ontvangers op de website van de Nationale Politie en het Openbaar Ministerie).
c. de doorwerking van art. 24a, lid 5, Wpg in art. 30 t/m 34 WvSv : de verstrekking van informatie bedoeld in de artikelen 24b (recht op informatie) 25, lid 1 (recht op inzage) 28, lid 1 (recht op rectificatie en vernietiging) vindt plaats overeenkomstige de artikelen 30 t/m 34 van het Wetboek van Strafvordering als de gegevens in een processtuk worden verwerkt. (het rapport van de deskundige van het NFI valt onder de processtukken).
d. de doorwerking van art. 39 ha, lid 3, Wjsg in de voornoemde artikelen 30 t/m 34 WvSv.
e. de doorwerking van art. 7 Wpg en art. 52 Wjsg (geheimhoudingsverplichting voor ontvangen politiegegevens, justitiële gegevens en strafvorderlijke gegevens voor het NFI.

C. Beschrijving en beoordeling risico's voor de betrokkenen

Beschrijf en beoordeel de risico's van de voorgenomen gegevensverwerkingen voor de rechten en vrijheden van de betrokkenen. Houd hierbij rekening met de aard, omvang, context en doelen van de gegevensverwerking zoals in onderdeel A en B zijn beschreven en beoordeeld. Het gaat hierbij overigens niet om de risico's van de verwerkingsverantwoordelijke zelf.

16. Risico's

Risico's en risicobeperkende maatregelen

Algemene risico's

Transparantie/rechten betrokkenen

De verwerking van persoonsgegevens van een betrokkene in een strafzaak is niet transparant. De betrokkene, zoals een verdachte, weet niet (altijd) dat zijn persoonsgegevens verwerkt worden. Daardoor kan de betrokkene ook geen inzicht krijgen in bijvoorbeeld de juistheid van zijn persoonsgegevens. Daarnaast kunnen er in een strafzaak ook persoonsgegevens verwerkt worden van personen die niets met het onderzoek te maken hebben (zogenaamde "bijvangst"). Deze personen kunnen dan ook geen gebruik maken van de rechten die aan hen toekomen op grond van de AVG. Voor de waarheidsvinding in (straf)zaken is het namelijk van groot belang dat er niet te *weinig* gegevens verzameld worden, omdat er juist zo'n volledig mogelijk beeld gecreëerd moet worden van een situatie/verdachte, overigens ook ter ontlasting van de verdachte. Alle gegevens die in Hansken verwerkt worden zijn noodzakelijk voor het bereiken van het doel, juist omdat er gezocht wordt naar schakels in een proces die kunnen dienen als bewijsmateriaal. Van te voren is niet altijd vast te stellen om welke/wat voor soort gegevens en om welke betrokkenen het gaat. De informatieplicht jegens betrokkenen, inzake de verwerking van persoonsgegevens in een strafzaak, wordt door Politie en het OM/RC vorm gegeven door het verstrekken van informatie via hun website omdat zij optreden als opdrachtgever richting NFI en omdat zij uiteindelijk bepalen of een betrokkene inzage in zijn data kan krijgen.
Bij verzoeken van betrokkenen voor inzage zal veelal een beroep worden gedaan op uitzonderingsgronden in de UAVG, artikel 41, lid 1, sub d. Op speciaal verzoek van de vertegenwoordiger van de verdachte (advocatuur) kan inzage worden gegeven in de chain of evidence of in uitzonderlijke situaties wordt de data in 'datarooms' inzichtelijk gemaakt. Dit is een separate Hansken instantie.
In algemene zin is de verwerking van persoonsgegevens door het NFI toegelicht op de website van het NFI. Het privacy statement zal echter nader uitgewerkt moeten worden.

Risico's **voor** het nemen van de risicobeperkende maatregelen:

Kans (laag, middel hoog)	**Impact** (laag, middel, hoog)	**Risico** (laag, middel, hoog)
M	M	M

Risicobeperkende maatregelen
Omdat de betrokkenen vaak niet in staat gesteld kunnen worden om hun rechten uit te oefenen, is het van groot belang dat de werkzaamheden onderworpen worden aan (externe) controle. Dat is in het Wetboek van Strafvordering voorzien. Daarnaast zou een (externe) audit gehouden kunnen worden om het risico voor betrokkenen verder te verkleinen.

De website van het NFI moet voorzien in een heldere uitleg over het gebruik van persoonsgegevens in relatie tot forensisch onderzoek in het kader van strafzaken. Hierbij kan ook gewezen worden op beroepsmogelijkheden en mogelijke ondersteuning door de Autoriteit Persoonsgegevens.

Dit risico voor betrokkene accepteren we omdat we een beroep kunnen doen op de wet de UAVG, artikel 41, lid 1, sub d.
En omdat de toegang tot de data van betrokkene beperkt is tot een kleine groep medewerkers die een geheimhoudingsverklaring ondertekend hebben en gescreend zijn door de AIVD.

Risico's **na** het nemen van de risicobeperkende maatregelen:

Kans (laag, middel hoog)	**Impact** (laag, middel, hoog)	**Risico** (laag, middel, hoog)
M	M	M

Bewaartermijnen

Er zijn ten aanzien van Hansken nog geen bewaartermijnen vastgesteld. Dit brengt het risico met zich mee dat data te lang bewaard wordt, voor andere doeleinden wordt gebruikt of dat de gegevens van de betrokkenen waarvan de zaak al is afgedaan nog steeds in de database zitten. Daarnaast heeft dit non-compliance tot gevolg, omdat het niet in overeenstemming is met de AVG om geen bewaartermijnen te hanteren. Incidenteel wordt op verzoek van de onderzoeker zaakdata vernietigd.

Risico's **voor** het nemen van de risicobeperkende maatregelen:

Kans (laag, middel hoog)	**Impact** (laag, middel, hoog)	**Risico** (laag, middel, hoog)
H	M	H

Risicobeperkende maatregelen
Dit risico kan beperkt worden door het vaststellen en hanteren van strikte bewaartermijnen. Het is te overwegen om de bewaartermijn cf de Wpg van maximaal 5 jaar aan te houden. Het is raadzaam om het verwijderen/vernietigen en archiveren van de gegevens niet handmatig maar automatisch te laten plaatsvinden. Ook voor back-ups, logging, onderzoeksrapporten en archiefmappen dienen bewaartermijnen te worden vastgesteld.

Risico's **na** het nemen risicobeperkende maatregelen:

Kans (laag, middel hoog)	**Impact** (laag, middel, hoog)	**Risico** (laag, middel, hoog)
L	M	L

Beveiligingsrisico's

Toegangs- en autorisatierisico's

Risico op schending van de privacy van betrokkenen. Alle medewerkers die Hansken technisch gezien gebruiken, hebben toegang tot de Hansken software. Autorisatie tot de data wordt verleend op zaakniveau. Dit gebeurt mondeling in overleg met de operators. Medewerkers van meerdere teams van het NFI kunnen bij het zaakmateriaal van Hansken als daarvoor toestemming is verleend. Er is tot op heden niet voldoende aandacht voor medewerkers die toegang krijgen tot bepaalde onderdelen in Hansken. Indien een medewerker van het NFI niet meer op een specifieke zaak wordt ingezet, worden de bevoegdheden over het algemeen niet ingetrokken. Het risico bestaat dat de gegevens ingezien kunnen worden door systeembeheerders of andere personen die niet bij de data zouden mogen komen. Er is geen stelselmatige controle op autorisaties. De toegangsrechten tot Hansken zijn verdeeld naar Lezen/toevoegen van markeringen/toevoegen van notities/aanpassen van status geheim gehouden data. Tevens is per rol aangegeven of de persoon acteert als: digitale rechercheur, tactisch rechercheur of als geheimhoudingsmedewerker.

Dit is al ontwikkeld door middel van de *role-based access* control: dit is een toegangscontrole waarbij de rechten worden gekoppeld aan rollen binnen de organisatie of bedrijfsproces. De individuen verkrijgen de rechten door een bepaalde rol te vervullen.

Daarnaast bestaat een *logging*: alle aanvragen op de centrale server, zoals autorisaties, aanvragen, data upload, forensische vragen, het opvragen van inhoud, etc., worden gelogd. Deze loggingen worden overgebracht naar een andere omgeving. Hierdoor is de logging afgescheiden voor de personen die toegang hebben tot Hansken en beschikt de logging over een eigen beveiligingssysteem. De logging kan per omgeving (NFI, Politie, etc.) worden geactiveerd.

Hansken heeft ook een Experimentele omgeving (losstaande instantie van Hansken). Toegang tot deze omgeving is vrij ruim opgezet en toegankelijk voor de meeste ontwikkelaars en enkele onderzoekers om nieuwe features/ontwikkelingen te toetsen (1 persoon met toegang tot de Experimentele omgeving is niet gescreend). In deze omgeving is dezelfde programmatuur en zaakdata beschikbaar als in de productie-omgeving en kunnen beveiligingsopties worden beïnvloed. De toegangsrechten in de productie- en experimenteer omgeving tot zaakdata zijn identiek ingericht.

Verder zijn de databronnen die zich in Hansken bevinden standaard versleuteld. Om de gegevens te ontsleutelen is er een digitale sleutel nodig, die per databron uniek is. Deze sleutel wordt buiten Hansken opgeslagen in de Keystore en moet worden aangeleverd bij het ophalen van gegevens. Voor beheerders (die geen toegang hebben tot de sleutel; dit is door het goed toekennen van rechten af te schermen) is het daardoor niet mogelijk om de gegevens in te zien. Het is echter wel zo dat degene met toegang tot de sleutel, deze sleutel met andere gebruikers kan delen wanneer dat nodig is. Het is daarom van belang dat vooraf goed wordt nagedacht over wie er toegang krijgen tot de sleutel en of geen beperking moet zitten aan de personen met wie deze sleutel gedeeld wordt. Recent is er een authenticatie op dit Hansken-component gezet, waardoor je alleen nog maar 'je eigen sleutels uit het sleutelkastje kan pakken'. Deze optie is voor de NFI omgeving operationeel.
De fysieke opslag van de data is nog *op een andere manier beveiligd, namelijk doordat* de disks van deze machines zijn versleuteld (bij diefstal van de schijven zijn de schijven onbruikbaar).
Hansken heeft een exportfunctie. Hiermee kunnen zaakdata buiten de beveiligde Hansken omgeving –onversleuteld- worden opgeslagen. De toegangsrechten tot deze exportdata zijn niet specifiek bepaald. Wel beperkt tot de medewerkers die toegang hebben tot de data directories van BDS.

Medewerkers die werken met Hansken (onderzoeker en ontwikkelaars) hebben een VOG en voor een groot deel van deze medewerkers zijn screenings uitgevoerd. Tevens heeft het NFI beveiligingsmaatregelen getroffen conform de BIR 2017.

Risico's **voor** het nemen van de risicobeperkende maatregelen:

Kans (laag, middel hoog)	**Impact** (laag, middel, hoog)	**Risico** (laag, middel, hoog)
H	M	M

Risicobeperkende maatregelen
Om de risico's tot schending van de privacy van betrokkenen te beperken, zijn de volgende maatregelen vereist:
De toegang tot zaakdata moet beperkt worden tot de data die een gebruiker daadwerkelijk nodig heeft en de procedures voor het verlenen van toegang tot een bepaalde zaak moeten worden geformaliseerd. Dit betreft ook de periodieke controle op de operationele toegangsrechten. Het is gewenst om de interne aanvraag- en afmeldprocedure voor toegangsrechten tot een zaak te formaliseren.
Toegang tot de Experimentele omgeving moet ingeperkt worden. Tevens dienen de rechten inzake beveiligingsopties in de Experimentele omgeving te worden ingetrokken. Dit geldt ook voor de nog te activeren laboratorium omgeving, zoals die in bijlage 2 is geschetst.

De monitoring op de logging moet nog worden ingeregeld.

Momenteel is de data binnen DBS ook via het netwerk te benaderen door onderzoekers. Als extra te nemen maatregel zou ingevoerd kunnen worden dat deze data-servers enkel door beheerders en door Hansken te benaderen zijn.

Medewerkers die werken met Hansken (onderzoeker en ontwikkelaars) hebben een VOG en voor een groot deel van deze medewerkers zijn screenings uitgevoerd. Aanbeveling is om het screenings% naar 100 % te brengen.

Een procedure opstellen om de toegang tot uit Hansken geexporteede zaakdata in te perken en deze data bij voorkeur encrypt op te slaan.

Risico's **na** het nemen van de risicobeperkende maatregelen:

Kans (laag, middel hoog)	**Impact** (laag, middel, hoog)	**Risico** (laag, middel, hoog)
L	M	L

Beschikbaarheid data

Het risico van verlies van data, waardoor voor een betrokkene mogelijk geen vrijspraak kan plaats vinden of onterecht een andere betrokkene als verdachte wordt aangemerkt.
Om de beschikbaarheid van de data ingeval van uitval van systemen, defecten, brand, etc. te waarborgen zijn additionele beveiligingsmaatregelen getroffen. Deze zijn verder niet beoordeeld. Waarborgen zijn vastgelegd in de SLA met het Rijkscomputercentrum en voor het NFI door het voldoen aan de BIR (actieplan voor compliance is onderhanden). Hansken draait op een Hadoop database met dubbele uitvoering van de data opslag. Overigens werkt Hansken o.b.v. een kopie van de originele data, waardoor de originele data nog steeds beschikbaar is voor een eventueel herstel.

Risico's **voor** het nemen van de risicobeperkende maatregelen:

Kans (laag, middel hoog)	**Impact** (laag, middel, hoog)	**Risico** (laag, middel, hoog)
L	L	L

Risicobeperkende maatregelen
Niet voorzien.

Datalek

Het risico van schending van de privacy van betrokkenen.
Bij elke verwerking van persoonsgegevens is er een kans op een datalek. Wanneer er een datalek ontstaat bij Hansken kan dit, door de hoeveelheid en privacy gevoeligheid van de gegevens, grote gevolgen hebben voor de betrokkenen van wie gegevens zijn verzameld. De impact voor de betrokkenen van wie persoonsgegevens gelekt zijn, kan vooral erg groot zijn als het gaat om bijzondere persoonsgegevens of strafrechtelijke gegevens. Daarnaast kan een datalek van de gegevens uit Hansken negatieve invloed hebben op de waarheidsvinding/het onderzoek. Denk bijvoorbeeld aan de situatie dat een verdachte door middel van een datalek erachter komt dat er heimelijk onderzoek naar hem gedaan wordt en hierdoor het onderzoek kan frustreren. Mogelijke datalekken zijn:

- Gegevens zijn ingelezen in het verkeerde zaakdomein
- De door Politie/OM aangeleverde datasets komen in onversleutelde vorm in handen van derden (slechts 5% is encrypt aangeleverd)
- Door onbevoegden is toegang verkregen tot de data in Hansken
- De encryptiesleutel is verloren gegaan
- Het onderzoeksrapport is naar de verkeerde bestemming gestuurd.

Reeds genomen maatregelen zijn het versleutelen van opgeslagen data in Hansken, waarbij de encryptiesleutel wordt opgeslagen in de Keystore Hansken. Na het inlezen van data worden verwerkingsverslagen aangemaakt. Deze worden vergeleken met data op het opdracht begeleidingsdocument. Daarnaast heeft het NFI beleid ten aanzien van (mogelijke) datalekken, waardoor een datalek zo snel mogelijk gesignaleerd wordt en de gevolgschade zoveel mogelijk wordt beperkt. Daarnaast zorgen technische en organisatorische beveiligingsmaatregelen ervoor dat de kans op een datalek zo klein mogelijk is.

Een verwerkersovereenkomst (waarin o.a. de verantwoordelijkheden en bevoegdheden zijn vastgelegd en hoe moet worden omgegaan met eventuele datalekken) met de RC is nog niet beschikbaar

Risico's **voor** het nemen van de risicobeperkende maatregelen:

Kans (laag, middel hoog)	**Impact** (laag, middel, hoog)	**Risico** (laag, middel, hoog)
L	H	M

Risicobeperkende maatregelen

Afspraak maken met toeleveranciers van inputdata, dat ze deze encrypt gaan aanleveren. En een check op de regels voor het versturen van rapporten aan opdrachtgevers met verificatie van de geadresseerde.
Het opstellen van een verwerkersovereenkomst met de Rc.

Riscio's **na** het nemen van de risicobeperkende maatregelen:

Kans (laag, middel hoog)	**Impact** (laag, middel, hoog)	**Risico** (laag, middel, hoog)
L	M	L

Functionele en kwaliteitsrisico's

Meer gegevens dan noodzakelijk

Het risico bestaat dat vertrouwelijke informatie van betrokkene wordt verwerkt (medische data, overleg met arts of advocaat) en dat gegevens van betrokkenen die geen rol spelen in de strafzaak worden verwerkt.
In de meeste strafzaken - en ook in Hansken – worden meer gegevens verzameld en verwerkt dan noodzakelijk is om het doel te bereiken. Wanneer het gaat om waarheidsvinding in (straf)zaken, zal veel informatie van belang zijn voor het onderzoek. Echter, van tevoren is lastig vast te stellen wat relevante informatie is en wat niet. Daarom zal er hoogstwaarschijnlijk meer data verzameld worden dan noodzakelijk is, waaronder ook data die wel betrekking heeft op de betrokkene en privacygevoelig is, maar niets te maken heeft met het onderzoek. Daarnaast kan er informatie verzameld en verwerkt worden van de verdachte die privacygevoelig is of bewijs is van een strafbaar feit, maar niet hetgeen waarnaar onderzoek wordt gedaan. Dit wordt 'bijvangst' genoemd.
Verder is het onvermijdelijk dat, door het grootschalig verwerken van data in strafzaken, ook data verzameld worden van derden die niets met het onderzoek te maken hebben; bijvoorbeeld van derde personen waarvan gegevens in de telefoon/laptop van verdachte staan.
Verder bestaat het risico dat er in de zaakdata ook informatie staat die niet mag worden gebruikt bij het onderzoek. Denk aan 'geheimhouderscommunicatie', zoals de communicatie tussen de verdachte en zijn advocaat.

Hansken heeft een aantal functionaliteiten waardoor er minder snel niet noodzakelijke gegevens bekeken worden. Dit is o.a. functionaliteit, die aan of uitgezet kan worden, waarmee bekende kinderporno gedetecteerd kan worden. Hiermee wordt voorkomen dat deze informatie, wanneer deze voor het onderzoek niet relevant is, gezien wordt door de onderzoekers.

Ook wat betreft het risico op het verwerken van hierboven genoemde 'geheimhoudingscommunicatie' bestaat een risicobeperkende maatregel: Hansken bevat de functionaliteit om dergelijke sporen uit te sluiten van het onderzoek. Dit houdt in dat het mogelijk is om vooraf een lijst van woorden op te geven waarbij na verwerking van deze lijst alle sporen met voorkomens van een of meerdere woorden niet worden getoond aan gebruikers. In enkele gevallen is het mogelijk dat sporen ten onrechte niet herkend worden als geheim en dus niet worden gemarkeerd. Daarom is het ook mogelijk dat een rechercheur gedurende het onderzoek sporen aanmerkt als vertrouwelijk. Hierbij wordt het spoor direct verwijderd uit de zoekresultaten. Omdat het ook mogelijk is dat iets onterecht als geheimhoudingscommunicatie wordt aangemerkt, kan een persoon worden aangewezen als 'medewerker geheimhouders'. Deze persoon heeft de rechten om geheimhouders

communicatie in te zien. Daarnaast kan een spoor worden voorzien van een 'niet-geheimhouders kenmerk' dat door gebruikers niet weg te halen is.

Risico's **voor** het nemen van de risicobeperkende maatregelen:

Kans (laag, middel hoog)	**Impact** (laag, middel, hoog)	**Risico** (laag, middel, hoog)
M	L	L

Risicobeperkende maatregelen
Geen aanvullende maatregelen voorzien.

Profilering en geautomatiseerde besluitvorming

Het risico bestaat dat een betrokkene ten onrechte wordt aangemerkt als verdachte door profilering en/of geautomatiseerde besluitvorming. Het strafrechtelijk onderzoek wordt ondersteund door Hansken. Op grond van data in Hansken kunnen van verdachten of andere betrokkenen profielen worden samengesteld.
Aan de hand van bepaalde gegevens kunnen persoonlijke aspecten van natuurlijke personen worden geëvalueerd, zoals gedrag, locatie, etc. Een eventueel conclusie/besluit op basis van geprofileerde gegevens wordt door menselijke tussenkomst genomen (door rechercheur).

Risico's **voor** het nemen van de risicobeperkende maatregelen:

Kans (laag, middel hoog)	**Impact** (laag, middel, hoog)	**Risico** (laag, middel, hoog)
L	M	L

Risicobeperkende maatregelen
Geen aanvullende maatregelen voorzien.

Bewerkings- en/of selectieprogrammatuur is niet betrouwbaar

Hierdoor bestaat het risico dat een betrokkene ten onrechte wordt aangewezen als verdachte.
Er bestaat een kans dat de selectie programmatuur en herkenning van beelden niet goed functioneert. Dit kan resulteren in onjuiste weergave van de data of tot ten onrechte indicatie van het wel/niet voorkomen van bepaalde beelden (bv wapens of voertuigherkenning in images). De onderzoeker dient in zijn onderzoeksverslag een toelichting te geven op de uitgevoerde bewerkingen en opgegeven selecties. Hiermee voorziet de onderzoeker in een repeteerbaar spoor van evidence. De resultaten van beeldinterpretaties worden getoond aan de onderzoeker met daarbij een indicatie van de waarschijnlijkheid dat het een juiste interpretatie is. De onderzoeker dient zelf vast te stellen dat de interpretatie juist is en dient ook zelf conclusies te trekken. Hiermee kunnen false positives worden uitgesloten.

Softwareontwikkeling: het ontwikkelproces van Hansken is zo ingericht dat bij elke wijziging van de Hansken-programmacode door een ontwikkelaar, tenminste twee andere ontwikkelaars akkoord dienen te geven op de wijziging. Deze risicobeperkende maatregel is ook een belangrijke maatregel voor wat betreft de beveiligingsrisico's. Een acceptatietest door gebruikers is niet ingericht. Voordat een codewijziging wordt geaccepteerd, dienen alle aanwezige testsruns te slagen. Iedere test, een zogenaamde *unit test*, toont aan dat één specifiek onderdeel van Hansken naar verwachting functioneert.

Risico's **voor** het nemen van de risicobeperkende maatregelen:

Kans (laag, middel hoog)	**Impact** (laag, middel, hoog)	**Risico** (laag, middel, hoog)
L	H	M

Risicobeperkende maatregelen

De beschikbare programmatuur onderwerpen aan goede testcycli en waar mogelijk laten certificeren of gebruik maken van gecertificeerde modules.

Risico's **na** het nemen van de risicobeperkende maatregelen:

Kans (laag, middel hoog)	**Impact** (laag, middel, hoog)	**Risico** (laag, middel, hoog)
L	M	L

Datakwaliteit/integriteitsrisico's

Door het verliezen van data of onjuistheden in het inlezen van data loopt de betrokkene het risico dat ontlastende gegevens kwijtraken, waardoor hij niet wordt ontheven van verdenking of dat ten onrechte een andere betrokken wordt aangewezen als verdachte.

Er bestaat een kans dat fouten worden gemaakt bij het uploaden van de gegevens die uiteindelijk verwerkt worden of dat de gegevens niet juist of onvolledig zijn. De gevolgen van dergelijke fouten kunnen groot zijn voor de betrokkenen en voor de waarheidsvinding. De gegevens worden ge-upload in Hansken of aan het NFI overgedragen en door het NFI in Hansken gezet. Het is van belang dat in het gehele proces secuur en zorgvuldig met de gegevens om wordt gegaan: zowel bij het vergaren van gegevens door derde partijen als bij het overzetten in Hansken. Allereerst wordt van de aangeleverde gegevens een exacte kopie gemaakt, waar mee gewerkt gaat worden. Het originele aangeleverde bestand bij de aanvrager wordt bewaard, buiten de scope van Hansken. Na het inlezen van de data vindt een vergelijking plaats van de ingelezen datasets met de op het opdrachtformulier beschreven datasets (géén controle op omvang of hashtotals).

Ook kunnen verkeerde conclusies getrokken worden uit de data door onvoldoende kennis van de tooling en de mogelijke interpretatie van getoonde resultaten. Programma's of tooling kunnen van onvoldoende kwaliteit zijn waardoor de kwaliteit van de uitkomsten onvoldoende kan zijn.

Verder is het ook mogelijk dat gebruikers zelf data (labels of notities) toevoegen aan sporen in Hansken. Het risico op foutieve of onvolledige data wordt zo veel mogelijk beperkt doordat er een onderscheid gemaakt wordt tussen metadata in Hansken en toegevoegde elementen door gebruikers. Bij deze functionaliteit wordt ook de *chain of evidence* bewaakt doordat geadministreerd wordt wie wanneer welke data toevoegt. Hansken voorziet in een logging van uitgevoerde handelingen in meerdere logfiles (de logs bevatten gebruikersverzoeken, interne server communicatie (niet inhoudelijk) en foutmeldingen). De bewaartermijn van de logfiles is niet vastgesteld en ze worden nu maar 1 week bewaard. Een verbetervoorstel is opgesteld, waarbij alle gebruikersacties op de REST-interface van Hansken worden gelogged. Dit gaat ook de raadpleging van data door gebruikers en acties van systeembeheerders loggen

Alle logging zal in een centraal systeem worden opgeslagen (een z.g.n. security information and event management systeem (SIEM)). Hier zal standaardsoftware worden gebruikt. Het SIEM zorgt er voor dat logs worden verwijderd als de bewaartermijn is verlopen, en dat enkel geautoriseerde personen bij de logging kunnen.

De Deskundige brengt een eindverslag uitbestemd voor de opdrachtgever. De bevindingen en conclusies in het rapport worden getoetst door een 2e deskundige (mede met behulp van het waarnemingsrapport (waarin alle uitgevoerde handelingen en zoekopdrachten zijn vastgelegd).

Daarnaast zijn er een aantal andere maatregelen die het risico's wat betreft datakwaliteit en integriteit zo klein mogelijk houden. Zo kunnen gebruikers sporen niet verwijderen. Verder zijn hier van belang:

- Opleidingen: voordat een gebruiker Hansken gebruikt, wordt aangeraden om de gebruiker een Hansken training te laten volgen. Deze training wordt verzorgd door het NFI en de politieacademie. De gebruiker krijgt door deze training inzicht in het digitaal forensisch onderzoek en digitale sporen.

- Voordat een nieuwe versie van Hansken wordt vrijgegeven voor productie, wordt naast de losse onderdelen ook de correcte werking van de gehele dienst getest. Hierbij wordt de dienst Hansken opgestart in een omgeving die vergelijkbaar is met de productie-omgeving. Vervolgens worden zogenaamde *integratietests* uitgevoerd die de dienst testen. Hierbij geldt dat één falende test er voor zorgt dat een onderzoek naar de oorzaak wordt ingesteld en de nieuwe versie niet wordt vrijgegeven voor productie.

Risico's **voor** het nemen van de risicobeperkende maatregelen:

Kans (laag, middel hoog)	**Impact** (laag, middel, hoog)	**Risico** (laag, middel, hoog)
L	M	M

Risicobeperkende maatregel

Controle van de resultaten: het is niet ondenkbaar dat er fouten worden gemaakt bij het inlezen van de data. Wij adviseren om controlegetallen of hashtotals toe te voegen bij aanlevering van de in te lezen data om de volledigheid van aangeleverde data te waarborgen.

Het uitvoeren van het verbetervoorstel voor de logging en het vaststellen van een passende bewaartermijn van de logfiles. Tevens bepalen hoe monitoring op de logging gaat plaatsvinden.

Risico's **na** het nemen van de risicobeperkende maatregelen:

Kans (laag, middel hoog)	**Impact** (laag, middel, hoog)	**Risico** (laag, middel, hoog)
L	M	L

Onrechtmatig datagebruik

Het risico bestaat dat door onrechtmatig gebruik van data of hacking gegevens worden gemanipuleerd waardoor een betrokkene ten onrechte wel/niet wordt aangewezen als verdachte in een strafzaak.

Het risico bestaat dat er onrechtmatig gebruik wordt gemaakt van de gegevens die in Hansken verwerkt worden. Onrechtmatig gebruik kan bijvoorbeeld voorkomen wanneer een medewerker van het NFI (of een hacker) de waarheidsvinding of het (straf)proces wil frustreren. Als iemand 'kwaad' wil met dergelijke gegevens dan kan dit van grote invloed zijn op de betrokkenen of de waarheidsvinding. Daarnaast kan er door onwetendheid, of per ongeluk, onrechtmatig gebruik gemaakt worden van de data.

Om dit risico zo klein mogelijk te houden is het ten eerste van belang dat de medewerkers van het NFI altijd in het bezit zijn van een VOG. Verder hebben de medewerkers van het NFI een geheimhoudingsverplichting. Daarnaast is het belangrijk om alleen de personen toegang te verschaffen die daadwerkelijk bij de gegevens moeten kunnen. Dit wordt op dit moment bij het NFI gedaan door het *role-based access model*. Dit betekent dat een gebruiker alleen iets mag in Hansken, als hij daarvoor expliciet toestemming heeft. Tevens heeft het NFI beveiligingsmaatregelen ingericht volgens de BIR 2017. De meeste gebruikers van Hansken zijn gescreend door de AIVD.

Risico's **voor** het nemen van de risicobeperkende maatregelen:

Kans (laag, middel hoog)	**Impact** (laag, middel, hoog)	**Risico** (laag, middel, hoog)
M	H	H

Risicobeperkende maatregelen.

Voor medewerkers die toegang hebben tot Hansken zal aanvullend de eis gesteld moeten worden dat er altijd Screening moet zijn uitgevoerd alvorens ze toegang te verlenen tot Hansken programmatuur en/of zaakdata. Er zal echter meer aandacht besteedt moeten worden aan wie wanneer (met welke rol) toegang krijgt tot welke gegevens/functies in Hansken. Daarnaast zou gedacht kunnen worden aan logging van mutaties in de audittrail (spoor van evidence), logging van toegang en hierop afgestemde monitoring door een onafhankelijke functionaris.

Risico's **na** het nemen van de risicobeperkende maatregelen:

Kans (laag, middel hoog)	**Impact** (laag, middel, hoog)	**Risico** (laag, middel, hoog)
L	H	M

D. Beschrijving voorgenomen maatregelen

In onderdeel D wordt bezien welke maatregelen kunnen worden getroffen om de in onderdeel C erkende risico's te voorkomen of te verminderen. Welke maatregelen in redelijkheid worden getroffen is een belangenafweging van de wetgever of verwerkingsverantwoordelijke. Voor dit onderdeel van de PIA is, als het gaat om beveiligingsmaatregelen, expertise over informatiebeveiliging belangrijk.

17. Maatregelen

Nr	Onderwerp	Voorgestelde maatregel	Belang	Follow-up
1	Transparantie/rechten betrokkenen	Periodieke audit op werkmethode Hansken	L	
2		Update van het privacy statement op de NFI website	H	
3	Bewaartermijnen	Het vaststellen van bewaartermijnen zaakdata in Hansken	H	
4	Toegang en Autorisatie	Formaliseren van toegangsverlening tot zaakdata voor NFI medewerkers formaliseren; dit geldt ook voor afmeldingen voor medewerkers die niet meer ingezet worden op een specifieke zaak	M	
5		Inperken bevoegdheden tot en in de zgn Experimenteer omgeving Hansken (niet kunnen uitschakelen van beveiligingsopties.	H	
6		Inrichting adequate logging en monitoring op logging van alle gebruikers activiteiten; en het bepalen van de bewaartermijn en van de logging	H	
7		Alle medewerkers die werken met Hansken moeten gescreend zijn	M	
8		Inrichten van de beveiliging van uit Hansken geexporteerde data.	H	
9	Datalekken	Input data door toeleveranciers versleuteld laten aanleveren	M	
10		Extra verificatie op adres van ontvanger rapportage	M	
11		Opstellen van een verwerkersovereenkomst met Rc	M	
12	Betrouwbaarheid programmatuur	De programmatuur / modules onderwerpen aan aantoonbare testcycli, en waar mogelijk laten certificeren	M	
13	Datakwaliteit	Toevoegen van maatregelen om de volledigheid en juistheid van het inlezen van aangeleverde data te waarborgen (bv door opnemen van hashtotals).	M	
14	Onrechtmatig datagebruik	Logging van alle mutaties in de audittrail in Hansken en inrichting bewaartermijnen en monitoring op deze logging	H	

E. Managementresponse

Onderdeel E bevat de managementrespons. Deze bestaat uit 2 delen:

- 1. Managementreactie DBS op PIA's Hansken: deze gaat met name in op de Hansken specifieke aspecten; d.d. 3 juli 2020 opgesteld door 10.2.e
- 2. Verslag van bespreking met het management van DBS, waarin de generieke aanbevelingen en acties voor digitaal onderzoek voor DBS staan beschreven. d.d. 29 juli 2020

1. Managementreactie DBS op PIA's Hansken (opgesteld door 10.2.e op 3 juli 2020 V1)

Inleiding

In 2019 zijn twee privacy impact assessments (PIAs) "zaakonderzoek met Hansken" uitgevoerd. In deze PIAs zijn maatregelen voorgesteld ter verbetering van de bescherming van persoonsgegevens en de eventueel nog uit te voeren vervolgonderzoeken.

In de aanbiedingsnota "Concept PIA zaakonderzoek door het NFI met Hansken" van 24 september 2019 is een lijst met 15 gegroepeerde aanbevelingen opgenomen. Deze nota bevat de managementreactie op deze aanbevelingen. Voor iedere aanbeveling is gekeken naar de *aanpassingen aan Hansken* en de aanpassingen op de DBS-omgeving en -processen.

In deze nota wordt verwezen naar meer gedetailleerde beschrijvingen voor uitbreidingen aan Hansken (HBACKLOG nummers, vastgelegd in JIRA) en naar NFI kwaliteits-documenten (QOL nummers, vastgelegd in Inception).

Er volgt eerst een algemene reactie. Vervolgens wordt voor iedere aanbeveling gekeken naar de Hansken-specifieke aspecten voor zowel het geven van inzicht in data als voor deskundigenrapportages en de daarbij benodigde aanpassingen aan Hansken. Tot slot worden 4 adviezen gegeven om de voorgestelde aanbevelingen op te volgen.

Algemene reactie

De twee uitgewerkte varianten vallen onder verschillende wettelijke regimes. Het is uit de PIA echter onvoldoende duidelijk wat de verschillen zijn met betrekking tot het soort onderzoek. Het NFI onderscheidt twee soorten onderzoek, namelijk onderzoek met en onderzoek zonder interpretatie van de resultaten binnen de zaakcontext. Dit lijkt overeen te komen met de varianten 1A (zonder interpretatie) en 1B (met interpretatie), de omschrijvingen van de varianten zoals omschreven in de PIA betreffen echter het juridische onderscheid, dat echter in de praktijk niet of nauwelijks een rol speelt en voor de praktijk ook geen relevant onderscheid is.

Variant 1A: Inzicht in data

De eerste PIA (variant 1A, *inzicht in data*) richt zich op zaakonderzoek met Hansken door het NFI als "forensisch onderzoeker" in opdracht van OM/politie. Dit betekent dat onderzoek op het NFI plaatsvindt om data inzichtelijk te maken ten behoeve van een specifieke zaak. Forensisch data-analisten, forensisch data scientists en/of forensisch software engineers voeren dit onderzoek uit onder aansturing van de

opdrachtgever. Het eindresultaat is inzicht in de data, waarbij het NFI dit resultaat niet binnen de context van de zaak interpreteert. Dit inzicht kan worden gegeven door middel van (a) een rapport, niet zijnde een deskundigenrapport, (b) een van de data afgeleide dataset of (c) een software-uitbreiding op forensische softwaretools (waaronder Hansken) en/of onderliggende forensische softwarebibliotheken.

De in de tabel op pagina 8 van deze PIA bij variant A genoemde opdracht "OM die de politie de Wpg data laat doorzoeken door het NFI" en product "analyse/ rapportage" komen niet helemaal overeen met bovenstaande toelichting. Het NFI doorzoekt de data niet, dat zou namelijk suggereren dat het NFI zaak-specifieke handelingen verricht waarvoor een deskundige de verantwoordelijkheid moet nemen (variant 1B).

Variant 1B: Deskundigenrapportage

De tweede PIA (variant 1B, *deskundigenrapportage*) richt zich op zaakonderzoek met Hansken door het NFI als "deskundige in strafzaken" in opdracht van het OM (als NRGD-geregistreerde deskundige) of een rechter. Forensisch data-analisten en data-scientists voeren dit onderzoek uit onder aansturing en verantwoordelijkheid van een bevoegd NFI-deskundige. Het eindresultaat is een forensisch rapport waarin op basis van vragen en hypothesen de data wordt wel geïnterpreteerd binnen de context van de zaak.

Forensisch deskundigenonderzoek aan digitaal materiaal is maatwerk. De werkmethoden hierbij zijn vastgelegd, o.a. voor kort onderzoek (QOL-02345) en maatwerkonderzoek (QOL-02350). Deze onderzoeken worden altijd geschaduwd (QOL-02355). Hansken is bij deze onderzoeken slechts één van de gereedschappen. Als Hansken gebruikt wordt, dan wordt dit gebruik gedetailleerd vastgelegd en gecontroleerd volgens NFI-brede kwaliteitsstandaarden.

Procedures voor de omgang met zaakdata

Zaakdata staat primair op zakenservers, maar deels ook op de computers van de betrokken onderzoekers. Dit is een punt dat voor het NFI algemeen van belang is en breder geadresseerd moet worden. Deze algemene punten worden door de privacy officer seperaat voorgelegd aan het MT NFI. Dit kan ook haast niet anders, deze computers zijn namelijk de forensische gereedschappen van de onderzoekers. Als Hansken als gereedschap gebruik.t wordt om inzicht te krijgen in (een deel van) de zaakdata, dan wordt deze data naar de Hansken-omgeving van het NFI gekopieerd.

Voor variant 1A waarbij een software-uitbreiding op Hansken of de door Hansken gebruikte bibliotheken wordt gemaakt, is de data primair beschikbaar op de computers van de betrokken medewerkers. Een kopie van deze data staat soms in Hansken.

Er moeten DBS-brede procedures worden opgesteld voor het bewaren van en toegang verlenen tot zaakdata op zowel de zakenservers als onderzoeksomgevingen, waaronder Hansken en computers van medewerkers. Deze procedure moet tevens vastleggen hoe en wanneer de zakenservers en gebruikte onderzoeksomgevingen geschoond moeten worden.

Transparantie en rechten betrokkenen

Periodieke audit op werkmethode Hansken

Belang: laag

De beschikbaarheid en toegankelijkheid van de benodigde zaakdata moet worden beschreven in de op te stellen procedures.

Het gebruik van Hansken voor zaakonderzoeken wordt expliciet vastgelegd in waarnemingen en gecontroleerd tijdens het schaduwen. Tegenonderzoek kan plaatsvinden zoals vastgelegd in de wet deskundigen in strafzaken.

Aanpassingen aan Hansken
Hansken wordt uitgebreid met een auditfunctie, de algemene werkzaamheden hiervoor zijn reeds gestart. Gedetailleerde specificaties voor deze functie worden vastgesteld in overleg met de Privacy Officer en Security Officer (HBACKLOG-16).

Update van het privacy'statement op de NFI website

Belang: midden
Het privacy statement is inmiddels aangepast.

Hansken zelf bevat meerdere onderdelen die impact hebben op de privacy van gebruikers of personen die voorkomen in de door Hansken inzichtelijk gemaakte zaakdata. Daarnaast bevat Hansken functies met als specifiek doel deze privacy te waarborgen, bijvoorbeeld door het verbergen van geheimhoudersinformatie. Om (medewerkers van) organisaties die Hansken (willen) gebruiken hierover goed te informeren, moet voor Hansken een privacy-statement worden opgesteld en beschikbaar gesteld aan de gebruikers.

Aanpassingen aan Hansken
Zodra een Hansken privacy statement beschikbaar is, wordt deze vanuit het platform beschikbaar gesteld. Op deze manier kan dit statement via de verschillende gebruikersinterfaces worden aangeboden aan eindgebruikers.

Bewaartermijnen

Het vaststellen van bewaartermijnen zaakdata in Hansken

Belang: hoog
Voor het maken van software-uitbreidingen is de zaakdata is nodig voor de duur van het onderzoek, d.w.z. voor tijd die nodig is om het inzicht in de data te realiseren. Bewaartermijnen moeten worden beschreven in de op te stellen procedures.

Een openstaande vraag is hoe we ervoor kunnen zorgen dat we goede testdata krijgen voor ontwikkelde software ten behoeve van onder andere unit- regressie- en integratietests? Dit kan niet op basis van de gebruikte zaakdata. Referentie-data creëren is niet altijd mogelijk.

Om zaakdata inzichtelijk te maken voor rapportage, het opleveren van datasets en deskundigenonderzoek, wordt een kopie ingeladen in het Hansken platform. De bewaartermijnen hiervoor moeten worden beschreven in de op te stellen procedures.

Aanpassingen aan Hansken
Hansken wordt uitgebreid met een functie die automatische waarschuwt wanneer zaakdata een bepaalde tijd niet is benaderd. Deze notificatie kan worden gebruikt als trigger om zaakdata uit het systeem te verwijderen.

Toegang en Autorisatie

Formaliseren van toegangsverlening tot zaakdata voor NFI medewerkers; dit geldt ook voor afmeldingen voor medewerkers die niet meer ingezet worden op een specifieke zaak

Belang: midden
De zakenservers zijn momenteel toegankelijk voor alle (gescreende) geautoriseerde onderzoek-medewerkers. Autorisaties in Hansken hebben alleen betrekking op de (kopie van de) data in Hansken.

Autorisaties op de zakenserver en de gebruikte onderzoeksomgevingen moeten worden beschreven in de op te stellen procedures.

Autorisaties op de kopie van de zaakdata in Hansken moeten worden belegd bij de zaakverantwoordelijke (in plaats van de systeem operators). De zaakverantwoordelijke moet de autorisaties kunnen beheren (inzien en aanpassen). Autorisaties kunnen een einddatum hebben.

Aanpassingen aan Hansken

Hansken wordt uitgebreid met een auditfunctie op het autorisatie-beheer, zodat de Privacy Officer en/of de Information Security Manager bij incidenten kan inzien weet wie wanneer toegang had tot zaakdata, wat zijn of haar rechten waren en wie hiervoor verantwoordelijk was.

Inperken bevoegdheden tot de zgn. Experimenteer omgeving Hansken (niet kunnen beïnvloeden van beveiligingsopties)

Belang: hoog

De experimenteeromgeving is beschikbaar om software-uitbreiding toe te passen in een grootschalige omgeving op zaakdata. Deze experimenteeromgeving moet worden geschouwd als productie-omgeving. Dit betekent dat alle voorwaarden voor de productie-omgeving ook gelden voor deze omgeving. De experimenteer-omgeving dient te autoriseren tegen de autorisatie-service van de bijbehorende productie-omgeving. Dit dient in procedures vastgelegd te worden.

De experimenteeromgeving wordt gebruikt om software-uitbreidingen te testen in een grootschalige omgeving op grote dataverzamelingen. Zulke tests zijn nodig omdat software in grote omgevingen zich anders kan gedragen. Dit gebruik moet in bovengenoemde procedures vastgelegd worden.

Om zaakdata inzichtelijk te maken voor rapportage, het opleveren van datasets en deskundigenonderzoek, wordt de experimenteeromgeving gebruikt voor grootschalige toepassing van data-analyses die (nog) geen onderdeel uitmaken van officiële releases van Hansken. Dit gebruik moet in bovengenoemde procedures vastgelegd worden.

Aanpassingen aan Hansken

Hansken wordt uitgebreid zodat gebruikers expliciet toegang moeten krijgen tot door zaakonderzoekers toegevoegde gegevens. Dit om te voorkomen dat software engineers die niet aan de zaak werken, deze gegevens kunnen inzien.

Inrichting adequate logging en monitoring op logging van alle gebruikers activiteiten, en het bepalen van de bewaartermijn van de logging

Belang: hoog

Autorisaties en logging in Hansken hebben alleen betrekking op de (kopie van de) data in Hansken. Deze logging zegt niets over de toegang en het gebruik van de data, aangezien deze ook beschikbaar is via de zakenserver.

Aanpassingen aan Hansken

Zoals eerder gesteld moet Hansken worden uitgebreid met een auditfunctie op zowel het gebruik als het autorisatie-beheer. De Verantwoordelijke voor Hansken dient de hiervoor benodigde logging vast te stellen, met advies van de Privacy Officer.

De logging zal door Hansken worden aangeboden aan een Security Information & Event Management (SIEM) oplossing. Automatische handhaving van de bewaartermijn voor de logs zal in de SIEM-oplossing moeten worden geconfigureerd.

Alle medewerkers die werken met Hansken moeten gescreend zijn

Belang: midden
Momenteel is het DBS-beleid al dat medewerkers die zaakonderzoeken uitvoeren en/of ontwikkelen aan Hansken gescreend moeten zijn.

Inrichten van de beveiliging van uit Hansken geëxporteerde data c.q. het afschermen van de exportfunctie

Belang: hoog
Zowel voor het geven van inzage in zaakdata als het maken van deskundigen-rapportages is Hansken slechts één van de gereedschappen. Inzichtelijke data wordt regelmatig met andere tools aanvullend verwerkt voor rapportage-doeleinden of voor oplevering van datasets. De exportfunctie van Hansken is hierbij een essentieel onderdeel, dat overigens ook wordt gelogd middels de auditfunctie. Afschermen van deze functie staat haaks op dit werkproces en geeft geen bescherming. De data is namelijk al via andere wegen beschikbaar voor de betrokken onderzoekers.

Aanpassingen aan Hansken
In Hansken kunnen sporen worden gemarkeerd als geheimshoudersinformatie. Deze gegevens worden achtergehouden voor onderzoekers. Deze functie lijkt voor het NFI minder van belang omdat het NFI veelal aan de slag gaan met een dataset die aangeleverd is door de ketenpartners, waarin de ketenpartners deze eerste selectie reeds gemaakt hebben en waarbij aan het NFI een specifieke onderzoeksvraag wordt gesteld. Desondanks wordt wel nog nagegaan of het NFI dan toch juridisch nog verplicht is een filter te gebruiken ten aanzien de geheimhoudersinformatie. (Overigens zou dat dan niet alleen gelden voor Hansken maar ook voor allerlei andere digitale tools om informatie te doorzoeken.)

Voor onderzoeken bij ketenpartners waarbij toegang tot de data *alleen* via Hansken loopt, wordt aan Hansken een functie toegevoegd die ervoor zorgt dat sporen die zowel beschikbaar als achtergehouden gegevens bevatten, niet meer geëxporteerd kunnen worden. Dit zijn typisch containers, bijvoorbeeld e-maildatabases met daarin een of meerdere e-mails met geheimhoudersinformatie. Zo'n database kan dan niet meer uit Hansken geëxporteerd worden.

Datalekken

Input data door toeleveranciers versleuteld laten aanleveren

Belang: midden
Aanlevering van de data loopt normaliter via de standaard kanalen van het NFI, waaronder de "blauwe kratten". In sommige gevallen wordt de data via de politie-omgeving van Hansken die bereikbaar is vanuit het NFI.

Over de aanlevering van data voor zaakonderzoek zullen afspraken tussen het NFI en de ketenpartners gemaakt moeten worden. Dit zal gebeuren in verwerkersafspraken met de ketenpartners, aansluitend op de SLA. Hiervoor moet eerst nog een juridische complicatie worden opgelost. Dit traject staat los van de PIA Hansken.

Extra verificatie op adres van ontvanger rapportage

Belang: midden
Rapportage vindt plaats volgens de richtlijnen van het NFI. Controle op de oplevering maakt onderdeel uit van de schaduwprocedure.

Oplevering van software-uitbreidingen loopt via de gewone releaseprocedures van Hansken. Alleen geautoriseerde ketenpartners kunnen de releases te downloaden.

Opstellen van een verwerkersovereenkomst met OM/politie

Belang: midden

Voor zaakonderzoek is Hansken slechts een van de gereedschappen die niet in alle gevallen wordt gebruikt. Een verwerkersovereenkomst staat dan ook los van het gebruik van Hansken. Dit moet NFI-breed opgepakt worden voor zaakdata in het algemeen.

Betrouwbaarheid programmatuur

De programmatuur / modules onderwerpen aan aantoonbare testcycli, en waar mogelijk laten certificeren; formeel protocol opstellen

Belang: midden

Certificeren van de Hansken programmatuur als geheel is niet mogelijk, onder meer omdat deze gebruik maakt van onderliggende componenten die niet gecertificeerd zijn, zoals Hadoop en Elasticsearch.

Aanpassingen aan Hansken

Testen is al integraal onderdeel van het Hansken ontwikkelproces. In de Definition of Done van op te leveren software wordt expliciet opgenomen dat er voldoende tests met voldoende testdata aanwezig moeten zijn. Daarnaast worden er bij een release testrapporten beschikbaar gesteld voor unit-, integratie- en regressietests.

Datakwaliteit

Toevoegen van maatregelen om de volledigheid en juistheid van het inlezen van aangeleverde data te waarborgen (bv door opnemen van hashtotals)

Belang: midden

Bij het kopiëren van (zaak)data voor forensisch onderzoek wordt de integriteit bewaakt door het berekenen en vergelijken van zogenaamde hashtotals. Dit is al opgenomen in de procedures voor het uitvoeren van zaakonderzoek en wordt gecontroleerd in de schaduwprocedure.

De het maken van software-uitbreidingen is de integriteit ook van belang. De uiteindelijke zaak vindt echter niet plaats op de kopie die wordt gebruikt voor de ontwikkeling van de software.

Aanpassingen aan Hansken

In Hansken zijn functies toegevoegd om hashtotals te berekenen over geïmporteerde zaakdata. Deze hashtotals worden ook gerapporteerd in de via de Hansken gebruikersinterface beschikbare rapportagefunctie. Om vast te stellen of het plaatsen van zaakdata in Hansken correct is verlopen, kunnen operators deze hashtotals vergelijken met de hashtotals van de aangeleverde zaakdata.

Onrechtmatig datagebruik

Inrichten monitoring op logging

Belang: hoog

Autorisaties en logging in Hansken hebben alleen betrekking op de (kopie van de) data in Hansken. Deze logging zegt niets over de toegang en het gebruik van de data, aangezien deze ook beschikbaar is via de zakenserver.

Aanpassingen aan Hansken

Zoals eerder gesteld moet Hansken worden uitgebreid met een auditfunctie op zowel het gebruik als het autorisatie-beheer. De Privacy Officer van het NFI dient de hiervoor benodigde logging vast te stellen.

De logging zal door Hansken worden aangeboden aan een Security Information & Event Management (SIEM) oplossing. Monitoring op deze logging zal in de SIEM-oplossing geconfigureerd moeten worden.

Advies

Binnen de kaders van het zaakonderzoek dat wordt uitgevoerd op het NFI (K1) met Hansken, zijn in de aangeboden PIA's Hansken aanbevelingen gedaan ter verbetering van de bescherming van persoonsgegevens en de eventueel nog uit te voeren vervolgonderzoeken. Deze reactie bevat 4 adviezen om deze aanbevelingen op te volgen.

Advies 1. Stel DBS-brede procedures op voor omgang met zaakdata
Er moeten DBS-brede procedures worden opgesteld voor het bewaren van en het toegang verlenen tot zaakdata op zowel de zakenservers als onderzoeks-omgevingen, waaronder Hansken (ontwikkel-, test-, experimenteer- en productie-omgevingen) en de onderzoeksmachines en werkplekken van medewerkers. Deze procedures moeten tevens vastleggen hoe en wanneer de zakerservers en gebruikte onderzoeksomgevingen geschoond moeten worden. De Werkgroep Bewaren&Vernietigen stelt kaders op voor bewaartermijnen. De privacy officer maakt onderdeel uit van deze werkgroep. Hierover wordt momenteel overlegd met het OM en het departement. Daarna zullen met de divisies afspraken gemaakt worden over het implementeren hiervan.

Advies 2. Stel een Hansken privacy statement beschikbaar.
Hansken zelf bevat meerdere onderdelen die impact hebben op de privacy van gebruikers of personen die voorkomen in de door Hansken inzichtelijk gemaakte data. Daarnaast bevat Hansken functies met als specifiek doel deze privacy te waarborgen, bijvoorbeeld voor het verbergen van geheimhoudersinformatie. Om (medewerkers van) organisaties die Hansken (willen) gebruiken hierover goed te informeren, moet voor Hansken een privacy-statement worden opgesteld en beschikbaar gesteld aan de gebruikers.

Advies is het opstellen en beschikbaar stellen van dit statement binnen het programma OK Hansken in de programma opdracht 'communicatie'. Het beschikbaar stellen aan eindgebruikers van Hansken is opgenomen in advies 4.

Advies 3. Ketenpartners laten zelf een PIA Hansken uitvoeren
De uitgevoerde PIA's betreffen het gebruik van Hanskens voor zaakonderzoek op het NFI. De inzet van Hansken bij en door ketenpartners maakt hiervan géén onderdeel uit. Ketenpartners dienen dus zelf (ook) een PIA Hansken uit te voeren. Het Hansken privacy statetement kan hiervoor als input gebruikt worden. Gewenste aanpassingen aan Hansken om maatregelen na te leven kunnen in overleg worden opgenomen binnen de programma opdracht 'ontwikkelen/verbeteren software'.

Advies 4. Breid Hansken uit op basis van de voorgestelde maatregelen

Advies is om binnen het programma OK Hansken de voorgestelde aanpassingen op te nemen in de programma opdracht 'ontwikkelen/verbeteren software'. Onderstaande tabel bevat een overzicht van deze uit te voeren aanpassingen aan Hansken.

Onderwerp	Maatregel	Aanpassing Hansken
Transparantie en rechten betrokkenen	Periodieke audit op werkmethode Hansken	Auditfunctie op gebruik Hansken
Transparantie en rechten betrokkenen	Update van het privacy statement op de NFI website	Beschikbaar stellen Hansken privacy statement
Bewaartermijnen	Het vaststellen van	Automatische notificatie

	bewaartermijnen zaakdata in Hansken	wanneer zaakdata een bepaalde tijd niet is benaderd
Toegang en Autorisatie	Formaliseren van toegangsverlening tot zaakdata voor NFI medewerkers; dit geldt ook voor afmeldingen voor medewerkers die niet meer ingezet worden op een specifieke zaak	Audltfunctie op het autorisatie-beheer
Toegang en Autorisatie	Inperken bevoegdheden tot de zgn. Experimenteer omgeving Hansken (niet kunnen beïnvloeden van beveiligingsopties)	Expliciet autorisatie voor door zaakonderzoekers toegevoegde gegevens
Toegang en Autorisatie	Inrichting adequate logging en monitoring op logging van alle gebruikers activiteiten; en het bepalen van de bewaartermijn van de logging	Auditfunctie op gebruik Hansken; Logging van Hansken aanbieden aan een Security Information & Event Management (SIEM) omgeving
Toegang en Autorisatie	Alle medewerkers die werken met Hansken moeten gescreend zijn	-
Datalekken	Inrichten van de beveiliging van uit Hansken geëxporteerde data c.q. het afschermen van de exportfunctie	Uitbreiding van de afhandeling van geheimhouders-informatie
Datalekken	Extra verificatie op adres van ontvanger rapportage	-
Datalekken	Opstellen van een verwerkersovereenkomst met OM/politie	-
Betrouwbaarheid programmatuur	De programmatuur / modules onderwerpen aan aantoonbare testcycli, en waar mogelijk laten certificeren; formeel protocol opstellen	Testcoverage in Definition of Ready; Testrapporten beschikbaar stellen aan eindgebruikers
Onrechtmatig datagebruik	Inrichten monitoring op logging	Logging van Hansken aanbieden aan een SIEM omgeving

2. Besprekingsverslag generieke aanbevelingen voor DBS

Besprekingsverslag inzake generieke aanpak aanbevelingen uit PIA Hansken
Datum: 29 juli
Aanwezig: 10.2.e

1. Autorisaties:
   Het ideale model is als volgt: "De zaakverantwoordelijke/zaakcoördinator krijgt initiële toegangsrechten tot de zaakdata. Deze persoon kan vervolgens andere medewerkers toegang verlenen tot de zaakdata. De zaakverantwoordelijke blijft operationeel verantwoordelijk voor wat met zaakdata gebeurt. Hiertoe inzicht nodig in toegekende rechten en in de toegang door medewerkers tot de zaakdata." Toegang tot data verlenen en beheren in een complexe multidisciplinaire omgeving voor DBS is niet eenvoudig. Gewenst discretionary en mandatory access mechanisme. Dit uitgangspunt doo[10.2.e] op te laten nemen in het NFI informatiebeveiligingsbeleid.
2. Ontwikkeling van een nieuw autori[10.2.e]echanisme voor NFI door IV[10.2.e] is trekker van dit project. Autorisatie richt zich op toegangsverlening tot specifieke mappen[10.2.e]al info opvragen en[10.2.e]n contact brengen met DBS[10.2.e] Planning is niet bekend.
3. Autorisatie en toegangsbeveiliging:
   Om te komen tot een praktisch werkbare oplossing zullen use cases uitgewerkt worden voor een aantal varianten. Te starten met FPDA. Trekker van use cases is[10.2.e] zijn te benaderen voor ondersteuning bij de uitvoering.
4. Logging:
   File access logging is ingericht voor DBS. DBS wil aansluiten op SOC JenV. De omvang van de logdatasets is te omvangrijk. Dit vereist voorselectie/aggregatie door DBS.[10.2.e] s hiermee bezig[10.2.e]al de uitwerking en monitoring rules toetsen.
5. Bewa[10.2.e]ijnen:
   Generieke afspraken maken voor bewaar/vernietig termijnen van zaakdata. Uitgangspunt vormt het basisselectiedocument van het NFI. Om te bepalen of zaakdata vernietigd kan worden is statusinfo vereist vanuit het OM. Voor het inrichten van de bewaar- en vernietig termijnen sluit DBS aan bij het NFI project Bewaren&Vernietigen van het NFI getrokken door[10.2.e] zal dit met[10.2.e] en leiding DBS bespreken. Voor de inventarisatie van de huidige situatie en de implementatie van de gewenste situatie is waarschijnlijk extra beheer-capaciteit vereist. De voorgestelde maatregel voor signalering van langere periode niet gebruikte datasets vormt een aanvullend vangnet.
6. PIA Hansken definitief maken:
   [10.2.e]al door toevoeging van de managementresponse en de toegezegde uitwerking door divisieleiding[10.2.e] van voorstellen voor generiek DBS, de PIA Hansken 1.0 versie opstellen. Eerste afstemming hiervoor met[10.2.e]
7. Screening:
   Voor welke functies binnen het NFI is een screening VGB nodig[10.2.e] niet gescreend[10.2.e] [10.2.e] voert samen met P&O een inventarisatie uit en zal komen met een nieuwe lijst van vertrouwensfuncties binnen het NF[10.2.e] heeft de status van dit onderwerp opgevraagd.
8. Voortgangsbewaking van actiepunt[10.2.e]sken en DBS generiek:
   [10.2.e]al per tertaal voorafgaand aan de tertaalrapportage een voortgangsbespreking arrangeren met[10.2.e] Voorbereiding in samenwerking met[10.2.e]

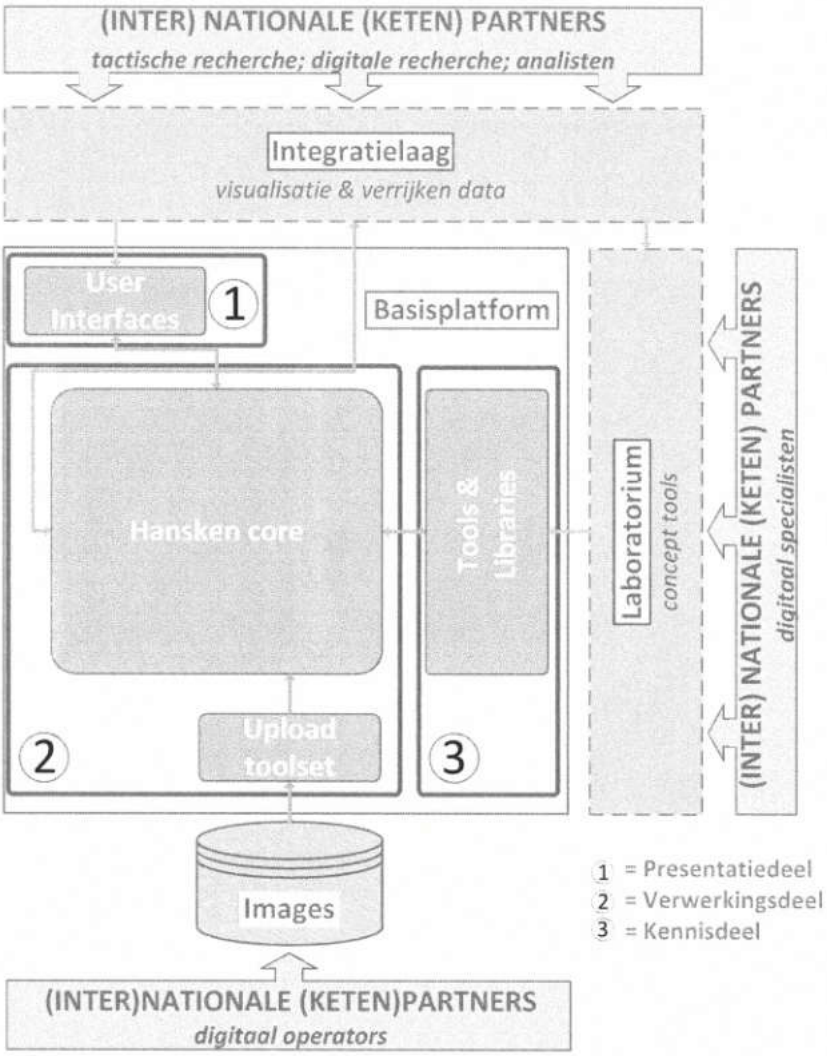
Bijlage I Het NFI als verantwoordelijke bij zaakonderzoek door NFI met Hansken in de rol van "deskundige in strafzaken"

Verantwoordelijke
Het NFI wordt gezien als "verantwoordelijke", en niet als "verwerker", omdat een verhouding verantwoordelijke – verwerker, waarbij bijvoorbeeld OM/RC of politie verantwoordelijke zou zijn en het NFI als verwerker zou optreden, zou impliceren dat OM/RC of politie aan het NFI *instructies zou geven* over de verwerking van de persoonsgegevens. Echter, het zeer specialistische werk dat NFI verricht voor deze ketenpartners wordt aan het NFI uitbesteed omdat het NFI nu juist bij uitstek over de hiervoor benodigde expertise beschikt. Dat brengt met zich mee dat het voor OM/RC en politie niet mogelijk is om het NFI deze instructies te geven. Dat maakt dat het NFI niet anders dan als "verantwoordelijke" kan worden gezien. Dit is in de aanloop naar 25 mei 2018 (van toepassing worden van de AVG) ook zo afgestemd en vastgesteld met OM, politie en ministerie van JenV.

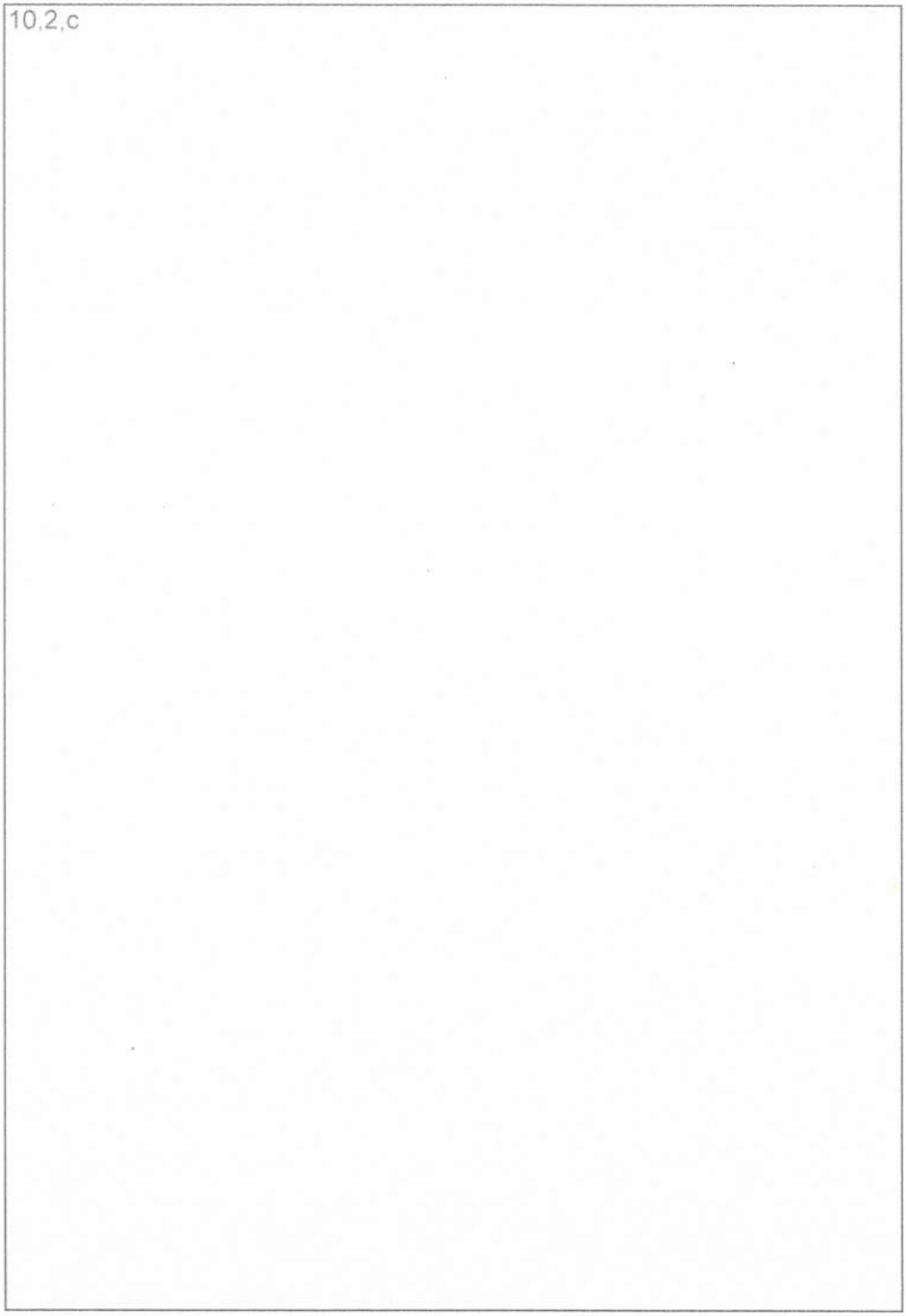
Gezamenlijke verantwoordelijkheid
Beter nog kan gesteld worden dat er sprake is van een "gezamenlijke verantwoordelijkheid" omdat OM en politie natuurlijk ook ieder verantwoordelijke zijn voor hun eigen verwerkingen van persoonsgegevens in het kader van de Wjsg en de Wpg. Wanneer de persoonsgegevens worden overgedragen aan het NFI, gaan ze onder het regime van de AVG vallen en na afloop van het onderzoek door het NFI, wordt het rapport of de uitkomsten weer aan het OM/RC gezonden, waar ze in het strafvorderlijke traject terechtkomen onder de Wjsg. Gezien deze verantwoordelijkheden over en weer is het noodzakelijk dat partijen onderling afspraken maken over de invulling van de gezamenlijke verantwoordelijkheid en duidelijk maken wie precies waarvoor verantwoordelijk is. Dit zal gebeuren door het maken van "verwerkersafspraken" die horen bij aan de Service Level Agreement (SLA) die het NFI sluit met politie en OM/RC, en overige Hansken-partners (Deze Hansken-SLA is separaat van de algemene SLA van het NFI met politie en OM over aantallen zaakonderzoeken, levertijden etc.).

Gezien deze verantwoordelijkheden over en weer is het noodzakelijk dat partijen onderling afspraken maken over wie precies waarvoor verantwoordelijk is. Dit zal gebeuren door het maken van "verwerkersafspraken" die horen bij aan de Service Level Agreement (SLA) die het NFI sluit met de RC. (Deze Hansken-SLA is separaat van de algemene SLA van het NFI met politie en OM over aantallen zaakonderzoeken, levertijden etc.).

Bijlage II Opbouw en functionaliteit Hansken en Processchema's Hansken



Bijlage III Processchema zaakonderzoek met Hansken



Bijlage IV Vakbijlage en procesbeschrijving Hansken

Inhoudsopgave

1. De vakbijlage algemeen
2. Inleiding
3. Beschrijving van het proces
3.1. Veiligstellen
3.2. Verwerking van de gegevens
3.3. Doorzoeken van sporen
4. Functionaliteit
4.1. Labels en notities
4.2. Rapportage
4.3. Geheimhouderscommunicatie
4.4. Eigen sporen toevoegen
5. Rolverdeling en verantwoordelijkheden
5.1. Verantwoordelijkheden
5.2. Gebruikersrechten
5.3. Sleutelbeheer
6. Kwaliteitsmaatregelen
6.1. Opleiding en bevoegdheden
6.2. Softwareontwikkeling
6.3. Tests
6.4. Controle van de resultaten
7. Verklarende woordenlijst
8. Literatuur

1. De vakbijlage algemeen

Sinds oktober 2015 biedt het Nederlands Forensisch Instituut (NFI) de dienst Hansken aan. Deze dienst ondersteunt het doorzoeken van (inbeslaggenomen) digitaal materiaal. Deze vakbijlage is ontwikkeld om als naslagwerk te dienen in een procesdossier. Deze vakbijlage dient als toelichting op de dienst en heeft een zuiver informatief karakter. De vakbijlage geeft weer hoe een onderzoek met behulp van Hansken in het algemeen plaatsvindt en welke aandachtspunten er bij een dergelijk onderzoek zijn. Aan het einde van de vakbijlage zijn een verklarende woordenlijst en een algemene literatuurverwijzing opgenomen.

2. Inleiding

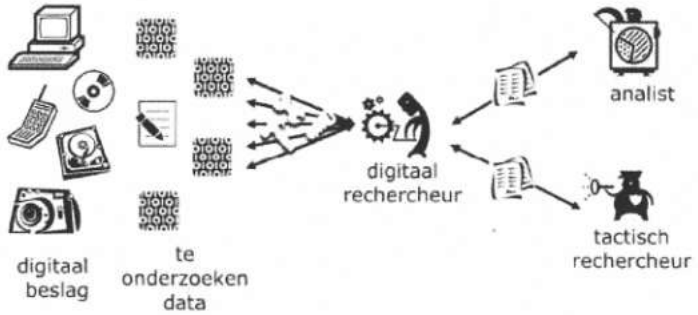
De hoeveelheid te onderzoeken gegevens en gegevensbronnen in strafzaken neemt razendsnel toe. Om de effectiviteit en snelheid van dit onderzoek te vergroten, heeft het Nederlands Forensisch Instituut (NFI) de forensische dienst Hansken ontwikkeld. Het doel van Hansken is om de juiste personen, op het juiste moment, toegang te geven tot de juiste informatie.
Met Hansken kan een onderzoeksteam snel en efficiënt zoeken in grote hoeveelheden in beslaggenomen gegevensdragers als computers en mobiele telefoons. Op alles wat relevant kan zijn, kan worden gezocht, bijvoorbeeld op woorden en namen of eigenschappen van *sporen* zoals chatberichten, e-mails of foto's al dan niet gemaakt met een bepaalde camera.
Rechercheurs kunnen met de forensische dienst de

zoekresultaten blijven filteren totdat je van die miljoenen sporen een selectie hebt, waarvan de sporen één voor één te bekijken zijn.

3. Beschrijving van het proces

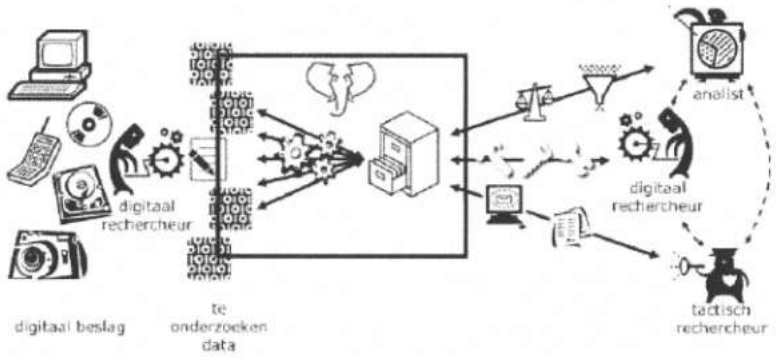
Hansken biedt een alternatief voor het traditionele proces voor digitaal forensisch onderzoek.

Figuur 1 Het traditionele proces voor het digitaal forensisch onderzoek



Figuur 1 geeft het proces weer zonder dat gebruik wordt gemaakt van Hansken. Hierbij is de digitaal rechercheur de persoon die het onderzoek uitvoert en hierover rapporteert aan degene die vragen heeft over het bewijsmateriaal (digitaal beslag).

Figuur 2 Het proces voor het digitaal forensisch onderzoek met gebruik van Hansken



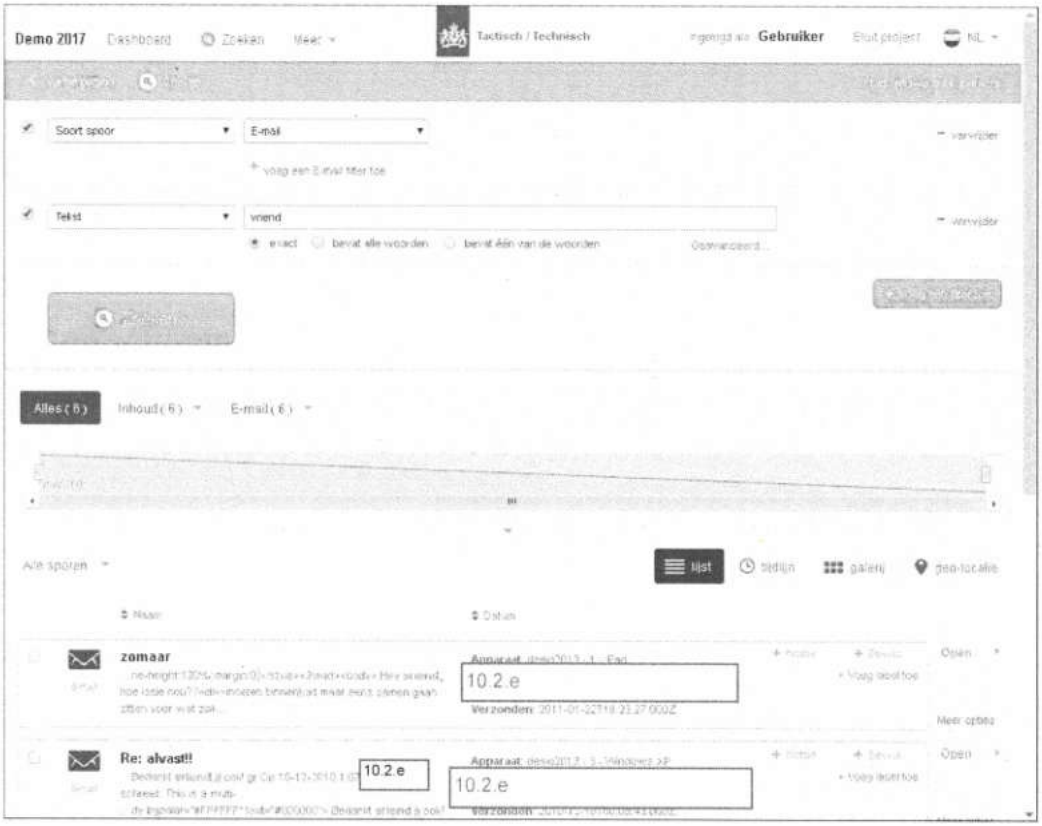
Figuur 2 toont het proces waarbij gebruik wordt gemaakt van Hansken. Hierbij is de digitaal rechercheur niet langer de centrale deelnemer maar kan de vraagsteller (tactisch rechercheur of analist) zelf in het digitaal bewijsmateriaal zoeken. Bij aanvullende vragen of de behoefte tot nadere duiding kan de digitaal rechercheur worden ingeschakeld.

3.1. Veiligstellen

Zoals bij elk digitaal forensisch onderzoek wordt begonnen met het maken van één-op-één-kopieën of een logische extractie van digitale bewijsmiddelen zoals van een harde schijf of een mobiele telefoon. Het veiligstellen gebeurt door de opdrachtgever volgens de hiervoor geldende procedures.

3.2. Verwerking van de gegevens

Bij de aanvraag van een Hansken-zaak levert de opdrachtgever informatie aan over een zaak, zoals de naamgeving en wie toegang mag krijgen tot de gegevens. De bij de zaak behorende veiliggestelde gegevens (bewijsbestanden) worden door de opdrachtgever naar Hansken geüpload of aangeleverd bij het NFI en door het NFI geüpload. Het is mogelijk om deze gegevens te voorzien van aanvullende (tactische) informatie, zoals de locatie waarop en/of persoon bij wie de gegevens zijn aangetroffen. Deze informatie wordt in Hansken bij de bewijsbestanden vastgelegd en kan later gebruikt worden bij het zoeken.
In Hansken worden bewijsbestanden (per zaak) samengevoegd in een *project*.
Vervolgens maakt Hansken structuren inzichtelijk die per project in één index worden vastgelegd. Per bewijsbestand vindt een extractie plaats waarbij herkenbare digitale objecten, ook wel *sporen* genoemd, uit het bewijsbestand worden gehaald. Voorbeelden zijn e-mails, chatgesprekken, PDF-documenten en digitale afbeeldingen.
Tijdens de extractie wordt een basisverzameling aan *tools* toegepast om zoveel mogelijk sporen uit de bewijsbestanden te halen. Enkele voorbeelden van dergelijke tools zijn tools die bestanden en mappen uit *bestandssystemen* halen, tools die logische rapportages van andere tools zoals UFED en XRY uitlezen, tools die e-mails en contactpersonen uit e-maildatabases lezen, tools die tekst uit afbeeldingen kunnen halen met *OCR* en tools die verwijderde bestanden kunnen terughalen. Deze verzameling kan op aanvraag uitgebreid worden met enkele specialistische tools. Op aanvraag verstrekt het NFI een overzicht van de beschikbare tools.



Wereldwijd wordt een grote diversiteit aan soft- en hardware gebruikt, wat zorgt voor een grote verscheidenheid aan sporen. Bij sporen van hetzelfde type kunnen verschillende eigenschappen worden opgeslagen. De eigenschappen die bij een e-mailbericht behoren zijn bijvoorbeeld anders als dit bericht wordt opgeslagen door Microsoft Office Outlook dan wanneer dit gebeurt door de standaard mailapplicatie op een iPhone.
De *tools* in Hansken vertalen deze verschillende vormen van sporen naar het uniforme datamodel voor Hansken, zodat deze later makkelijker doorzocht kunnen worden.

3.3. Doorzoeken van sporen

De sporen kunnen door een rechercheur, analist, forensisch onderzoeker of een andere belanghebbende worden doorzocht. Om een zoekvraag te stellen, wordt gebruik gemaakt van een specifiek voor Hansken ontwikkelde zoektaal. Deze zoektaal, de *Hansken Query Language*, is gebaseerd op een bestaande zoektaal, de *Lucene Query Language*.
Om de eindgebruikers te ondersteunen, zijn in samenwerking met eindgebruikers meerdere gebruikersinterfaces (*grafische user interfaces*) ontwikkeld. De twee belangrijkste zijn de tactische en de technische gebruikersinterface.

De tactische gebruikersinterface, gericht op tactisch rechercheurs, heeft als doel om informatie zo herkenbaar mogelijk te presenteren en om het zoeken eenvoudig te maken. Voor het gebruik van deze interface is dan ook de geen digitaal expertise nodig. Figuur 3 toont een voorbeeld van de tactische gebruikersinterface.
De technische gebruikersinterface geeft de rechercheur alle beschikbare informatie en biedt uitgebreide zoek- en presentatiemogelijkheden. De doelgroep van deze gebruikersinterface is de rechercheur die meer affiniteit heeft met digitaal forensisch onderzoek.
Zoeken met Hansken gebeurt door filters toe te passen op de sporen. Als geen filter wordt toegepast, worden *alle* sporen binnen het geopende project weergegeven. Hierbij is het mogelijk om sporen individueel te bekijken. Als de gebruiker een filter instelt, blijft het aantal sporen gelijk of wordt kleiner. Hierdoor is het mogelijk om snel en efficiënt in te zoomen op de revelante sporen. De ingestelde filters kunnen ook worden verwijderd of aangepast indien dit nodig is.

Figuur 3 voorbeeld van de tactische gebruikersinterface van Hansken

Voorbeelden van filters zijn zoekwoorden, datum- en tijdinformatie en eigenschappen van sporen (*metadata*), zoals de afzender van een e-mailbericht. Doordat binnen Hansken gebruik wordt gemaakt van een datamodel, kunnen deze filters op een uniforme manier worden ingesteld.
Bij het zoeken op woorden kan worden aangeven waar woorden moeten voorkomen en hoe woorden gecombineerd moeten worden. Er kan in de inhoud van sporen, in eigenschappen (metadata) of in beide gezocht worden. Daarnaast kan worden aangegeven of minstens één woord of alle woorden moeten voorkomen en of ze wel of niet in de opgegeven volgorde moeten staan. Ook op delen van woorden kan worden gezocht. Hansken is niet gevoelig voor hoofdletters of bijzondere leestekens. Woorden korter dan drie letters worden niet meegenomen.
De sporen in het zoekresultaat kunnen worden gesorteerd op relevantie met betrekking tot de zoekvraag1, datum en tijd of specifieke eigenschappen van de sporen.

4. Functionaliteit

Hansken biedt functionaliteit die specifiek is ontwikkeld om het onderzoeksproces te ondersteunen. In deze sectie wordt een aantal functionaliteiten nader beschreven.

4.1. Labels en notities

Als gedurende een onderzoek een spoor wordt gevonden waarbij de wens staat deze te markeren, is dit op twee manieren mogelijk. Ten eerste kan een label aan een spoor of set aan sporen worden toegekend. Labels zijn korte beschrijvingen van één of een aantal woorden waarbij verder geen informatie over bijvoorbeeld de auteur wordt vastgelegd. Met deze labels kunnen sporen worden gegroepeerd. Ten tweede kan een notitie aan een spoor worden toegevoegd. Hierbij kan meer informatie worden geplaatst en worden de auteur en het tijdstip bijgehouden. Voor zowel labels als notities geldt dat er meer dan één aan een spoor kan worden gekoppeld.

1 Relevantie wordt bepaald op basis van de tf/idf-score (term frequency inverse document frequency) van een spoor: de verhouding van de voorkomens van het woord in een spoor ten opzichte van de grootte van

het spoor en de voorkomens van het woord in de volledige index van de zaak.

4.2. Rapportage

Indien een spoor wordt aangetroffen waarvan het nuttig is de eigenschappen te rapporteren, is het mogelijk om een rapportage vanuit Hansken te genereren. Zo'n rapport bevat een feitelijke weergave van het spoor, d.w.z. de aangetroffen structuur die leidt tot het spoor én de aangetroffen metadata van het spoor zelf. Naast de eigenschappen van het spoor is het mogelijk om andere informatie op te nemen, zoals de notities en labels, de inhoud van het spoor en de versie van Hansken en de gebruikte tools.
De versie van Hansken en de gebruikte tools geven informatie over de plaats waarop het spoor in het bewijsbestand is aangetroffen. Dit is van belang voor de *chain of evidence*. Vanwege het continu verbeteren van de software is het mogelijk dat in latere versies van Hansken of van de tools andere of nieuwe sporen geïdentificeerd worden.

4.3. Geheimhouderscommunicatie

Onder geheimhouderscommunicatie wordt verstaan communicatie tussen de verdachte en een verschoningsgerechtigde zoals een arts of advocaat. Deze communicatie mag niet gebruikt worden in het onderzoek. Hansken bevat daarom functionaliteit om dergelijke sporen uit te sluiten van het onderzoek. De functionaliteit sluit aan op de werkwijze beschreven in de "Handleiding Verwerking geheimhouderinformatie aangetroffen in inbeslaggenomen voorwerpen en in digitale bestanden" van de Landelijke Vergadering Rechercheofficieren juni 2014.
In essentie houdt de functionaliteit in dat het mogelijk is om vooraf een lijst van woorden op te geven waarbij na verwerking van deze lijst alle sporen met voorkomens van een of meerdere woorden niet worden getoond aan gebruikers. In enkele gevallen is mogelijk dat sporen ten onrechte niet worden herkend als geheim en dus niet worden gemarkeerd. Daarom is het ook mogelijk dat een rechercheur gedurende het onderzoek sporen aanmerkt als vertrouwelijk. Hierbij wordt het spoor direct verwijderd uit de zoekresultaten.
Omdat het ook mogelijk is dat iets onterecht als geheimhouderscommunicatie wordt aangemerkt, kan een persoon worden aangewezen als "medewerker geheimhouders". Deze persoon heeft de rechten om geheimhouderscommunicatie in te zien en deze status van een spoor af te halen zodat het spoor weer in te zien is door rechercheurs.

4.4. Eigen sporen toevoegen

Het is mogelijk dat gebruikers zelf sporen toevoegen. Het datamodel van Hansken ondersteunt dit door onderscheid te maken tussen sporen toegevoegd door de Hansken *tools* en sporen toegevoegd door gebruikers. Bij deze functionaliteit wordt ook de *chain of evidence* bewaakt doordat geadministreerd wordt wie wanneer welke sporen toevoegt.

5. Rolverdeling en

verantwoordelijkheden

Het NFI heeft Hansken ontwikkeld in samenwerking met onder andere de Nationale Politie en de FIOD. Om de kwaliteit van zowel het onderzoeksproces als de dienst Hansken te garanderen, zijn er afspraken gemaakt over verantwoordelijkheden, opleiding, bevoegdheden en kwaliteit.

5.1. Verantwoordelijkheden

Het NFI is verantwoordelijk voor de programmacode van Hansken.
De politie beheert zelf de dienst Hansken inclusief de onderliggende infrastructuur, dat wil zeggen de hardware waar Hansken op draait en de benodigde systeemsoftware. Voor andere organisaties ligt de verantwoordelijkheid voor de dienst bij het NFI.
Het applicatiebeheer, zoals het aanmaken van projecten en het verwerken van bewijsbestanden, ligt in beide gevallen bij het NFI.
Op dit moment kan een aantal politie-eenheden zelf bewijsbestanden in Hansken plaatsen. De bedoeling is dat dit op termijn vanuit alle politie-eenheden mogelijk is.
De wensen voor nieuwe functionaliteiten komen bij de gebruikers vandaan en de verantwoordelijkheid voor het inplannen van deze wensen ligt bij het ontwikkelteam van het NFI. Het gebeurt regelmatig dat een specifiek onderzoek om specifieke functionaliteit vraagt. Het uitgangspunt van het NFI bij toevoegen van deze functionaliteit is dat het altijd dusdanig generiek dient te zijn dat het ook voor andere onderzoeken toegevoegde waarde heeft.

5.2. Gebruikersrechten

Het rechtenmodel van Hansken is ingericht volgens het *Rolebased access control*-model. In essentie komt dit model er op neer dat een gebruiker alleen iets mag, indien hij hier expliciet toestemming voor heeft. Voorbeelden van rechten zijn het mogen aanmaken van projecten, het mogen toevoegen van labels en het mogen inzien van geheimhouderscommunicatie. Door deze manier van toegang verlenen, is het niet mogelijk om een functie uit te voeren waarvoor de gebruiker geen toestemming heeft. Het toekennen van deze toestemming gebeurt door de applicatiebeheerder van Hansken.

5.3. Sleutelbeheer

Gegevens in Hansken worden versleuteld opgeslagen. Om deze gegevens te ontsleutelen, is een digitale sleutel nodig. Deze sleutel wordt opgeslagen buiten Hansken en moet worden aangeleverd bij het ophalen van gegevens. Het is voor beheerders van de omgeving (zonder toegang tot de sleutels) dan ook niet mogelijk om deze gegevens in te zien. Iemand die toegang heeft tot een sleutel, kan deze sleutel met andere gebruikers delen.

6. Kwaliteitsmaatregelen

Om de kwaliteit van de dienst en de daaruit voortvloeiende resultaten te waarborgen, is een aantal maatregelen genomen.

6.1. Opleiding en bevoegdheden

Voordat een gebruiker de dienst gebruikt, wordt sterk aangeraden de gebruiker een Hansken-training te laten volgen. Deze trainingen worden verzorgd door het NFI en de Politieacademie. Tijdens deze training krijgt de gebruiker inzicht in het digitaal forensisch onderzoek en digitale sporen. Ook gaat de gebruiker werken met Hansken, bij voorkeur in een operationele zaak.
Gebruikers die toestemming hebben om gegevens (bewijsbestanden) in Hansken te plaatsen, krijgen een gerichte instructie om zorg te dragen dat de infrastructuur van Hansken niet overbelast raakt.

6.2. Softwareontwikkeling

Het ontwikkelproces is zo ingericht dat bij elke wijziging van de Hansken-programmacode door een ontwikkelaar tenminste twee andere ontwikkelaars akkoord op de wijziging dienen te geven. Onderdeel van de *best practices* bij codeontwikkeling is dat de wijzigingen worden ondersteund door bijbehorende tests die de functionaliteit aantoont.

6.3. Tests

Voordat een codewijziging wordt geaccepteerd, dienen alle aanwezige tests te slagen. Iedere test, een zogenaamde *unit test*, toont aan dat één specifiek onderdeel van Hansken naar verwachting functioneert.
Voordat een nieuwe versie van Hansken wordt vrijgegeven voor productie, wordt naast de losse onderdelen ook de correcte werking van de gehele dienst getest. Hierbij wordt de dienst Hansken opgestart in een omgeving die vergelijkbaar is met de productieomgeving. Vervolgens worden zogenaamde *integratietests* uitgevoerd die de dienst testen. Hierbij geldt dat één falende test er voor zorgt dat een onderzoek naar de oorzaak wordt ingesteld en de nieuwe versie niet wordt vrijgegeven voor productie.

6.4. Controle van de resultaten

Hoewel bij het testen over het algemeen de belangrijkste fouten worden achterhaald, is het niet ondenkbaar dat in productie toch fouten optreden. Hierbij zijn twee soorten fouten te onderscheiden: resultaten kunnen onvolledig zijn en resultaten kunnen incorrect zijn. Na een extractie wordt door de operationeel beheerders een aantal standaardresultaten bekeken om te bepalen of de extractie naar verwachting is verlopen. Bij een onverwachte afwijking wordt onderzoek ingesteld naar de oorzaak en wordt de opdrachtgever geïnformeerd over de afwijking.
Gebruikers worden er, bijvoorbeeld tijdens de opleiding, op gewezen dat resultaten die van belang zijn voor het onderzoek altijd dienen te worden gecontroleerd met andere software. Hiervoor kunnen zij zich wenden tot een digitaal rechercheur. Dit is ook verstandig indien onduidelijkheid bestaat over de resultaten. Het NFI schrijft niet voor hoe over sporen moet worden geverbaliseerd, aangeraden wordt om dit zo veel mogelijk in samenwerking met een digitaal rechercheur te doen.

7. Verklarende woordenlijst

Best practice Een in de praktijk toegepaste techniek, methode of manier van werken die aantoonbaar zeer goed

functioneert.
Chain of evidence De chain of evidence legt zo gedetailleerd mogelijk vast wat er met onderzoeksmateriaal is gebeurd en/of hoe het tot stand is gekomen, vanaf het eerste moment waarop het onderdeel werd van een onderzoek.
Metadata Data over data, bijvoorbeeld de naam van een bestand, de afzender van een e-mailbericht of het merk camera waarmee een digitale foto is gemaakt.
OCR Optical Character Recognition (OCR), in het Nederlands optische tekenherkenning, is een techniek waarbij uit een digitale afbeelding door middel van patroonherkenning tekst wordt gehaald.
Project Een met Hansken doorzoekbare verzameling gegevens (bewijsbestanden), in de praktijk vaak overeenkomend met de gegevens binnen één (straf)zaak.
Role-based access control Toegangscontrole, waarbij rechten worden gekoppeld aan rollen binnen een organisatie of bedrijfsproces. Individuen verkrijgen de rechten door een bepaalde rol te vervullen.
Sporen Voor gebruikers herkenbare digitale objecten, bijvoorbeeld e-mails, chatberichten, digitale afbeeldingen, opgemaakte tekstdocumenten en spreadsheets.
Tools Gereedschappen die tijdens de extractie gebruikt worden voor de analyse van specifieke digitale sporen met als doel deze sporen te verrijken en/of nieuwe sporen uit deze sporen te extraheren. Een overzicht van de beschikbare tools is op te vragen bij het NFI.

8. Literatuur

In de vakbijlage zijn geen expliciete verwijzingen gebruikt naar literatuur, aangezien het eigen ontwikkelde programmatuur betreft. Over het veranderende proces en de manier hoe dit in Hansken is vormgegeven zijn twee publicaties geschreven die goed als referentie te gebruiken zijn:

1. Van Baar, R. B., Van Beek, H. M. A. en Van Eijk, E. J. "Digital Forensics as a Service: A game changer." *Digital Investigation* 11 (2014): S54-S62.2, beschikbaar op https://doi.org/10.1016/j.diin.2014.03.007
2. Van Beek, H. M. A., et al. "Digital forensics as a Service: Game on." *Digital Investigation* 15 (2015): 20-38, beschikbaar op https://doi.org/10.1016/j.diin.2015.07.004

Voor algemene vragen kunt u contact opnemen met de Frontdesk, telefoon (070) 888 68 88. Voor inhoudelijke vragen kunt u contact opnemen met de divisie Digitale en Biometrische Sporen telefoon (070) 888 64 00.
Nederlands Forensisch Instituut
Ministerie van Justitie en Veiligheid
Postbus 24044 | 2490 AA Den Haag
Telefoon (070) 888 66 66
www.forensischinstituut.nl

Bijlage V Memo grondslagen NFI

MEMO

Grondslagen voor primaire verwerkingen van persoonsgegevens

van het

Nederlands Forensisch Instituut

Projectteam Implementatie AVG
Auteur 10.2.e

Mei 2018
Versie 0.1

1. Inleiding en achtergrond

Met ingang van 25 mei 2018 zijn de Algemene Verordening Gegevensbescherming (AVG) en de Uitvoeringswet AVG (UAVG) van toepassing op de verwerkingen van persoonsgegevens van het NFI.

Door het NFI worden ten behoeve van zijn kerntaken drie van elkaar te onderscheiden typen persoonsgegevens verwerkt:

1. gewone persoonsgegevens: naam, adres woonplaats, etc.
2. bijzondere persoonsgegevens: gegevens die betrekking hebben op ras of etnische afkomst, politieke opvattingen, religie of levensbeschouwelijke overtuiging, lidmaatschap van een vakbond, genetische gegevens, biometrische gegevens met het oog op iemands unieke identificatie, iemands gezondheid, of iemands seksueel gedrag of seksuele gerichtheid. Deze persoonsgegevens zijn privacygevoeliger dan gewone persoonsgegevens. Lichaamsmateriaal valt ook onder dit type.
3. strafrechtelijke persoonsgegevens: strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen.

Voor het verwerken van die typen persoonsgegevens heeft het NFI als verwerkingsverantwoordelijke[8] een wettelijke grondslag nodig. Eén van de actiepunten in het Plan van Aanpak Implementatie AVG is het verschaffen van duidelijkheid over de grondslagen waarop het NFI persoonsgegevens verwerkt voor zijn kerntaken.[9]

2. Doel memo

Het doel van deze memo is het beantwoorden van de volgende vragen:

1. *Voor welke specifiek doelen verwerkt het NFI persoonsgegevens?*
2. *Op welke grondslagen verwerkt het NF gewone persoonsgegevens?*
3. *Op welke grondslagen verwerkt het NFI bijzondere en strafrechtelijke gegevens?*[10]
4. *Zijn deze grondslagen toereikend voor de geïnventariseerde primaire verwerkingen van persoonsgegevens van de NFI?*

Buiten het bestek van deze memo vallen de grondslagen voor de verwerkingen in opdracht van het Caribisch deel van het Koninkrijk der Nederlanden.[11] Hiervoor is een afzonderlijke memo bij het team Juridische Zaken in voorbereiding.

3. Beantwoording van de vragen

3.1 Doel van de primaire verwerkingen van het NFI

[8] De Minister van Justitie en Veiligheid is formeel de verwerkingsverantwoordelijke zoals bedoeld in art. 4, sub 7, AVG. De Directeur van het NFI is namens de Minister de beheerder van de verwerkingen.

[9] Het NFI kan in voorkomende gevallen, afhankelijk van een specifieke opdracht voor een product of dienst, als verwerker in de zin van art. 4, sub 8, AVG optreden. Afhankelijk van de soort opdrachtgever kan dan de grondslag art. 28 AVG of art. 22 Richtlijn Opsporing en Vervolging zijn. Deze grondslagen zijn in die gevallen toereikend en dit valt verder buiten het bestek van deze memo.

[10] Formeel: persoonsgegevens van strafrechtelijke aard (zie art. 1 UAVG).

[11] Het Caribisch deel van het Koninkrijk der Nederlanden bestaat uit: de landen Aruba, Curaçao en Sint Maarten en de 3 openbare lichamen Bonaire, Sint Eustatius en Saba.

De naam van de verwerking van persoonsgegevens ten behoeve van de kerntaken is gelijkluidend aan het zakenregistratiesysteem Promis. Het register van verwerkingsactiviteiten van het NFI vermeldt voor de primaire verwerking Promis de volgende doelen:

Het verwerken van persoonsgegevens ten behoeve van:

A. *de ondersteuning van de kerntaken van het NFI met het oog op de waarheidsvinding in strafzaken:*
   1. *het verrichten van onafhankelijk forensisch zaakonderzoek op overwegend technisch, medisch-biologisch en natuurwetenschappelijk gebied en het ter zake daarvan uitbrengen van verslag;*
   2. *het ontwikkelen en implementeren van nieuwe onderzoeksmethoden en technieken ter bevordering van kennis op het gebied van forensisch onderzoek;*
   3. *het zijn van (inter)nationaal kennis- en expertisecentrum op het gebied van het forensisch onderzoek.*

B. *het leveren van producten en diensten die in het verlengde liggen van die kerntaken en een onlosmakelijke samenhang hebben met de waarheidsvinding in strafzaken:*
   1. *activiteiten die bijdragen aan de handhaving van de (inter)nationale rechtsorde of veiligheid en waarvan het om redenen van kwaliteit, zorgvuldigheid, doelmatigheid, continuïteit of herkenbaarheid wenselijk is dat het NFI deze verricht;*
   2. *de ondersteuning bij de hulpverleningstaak van de politie, bedoeld in artikel 2 van de Politiewet 1993.*

B. *het leveren van andere producten en diensten ingeval van zaken van groot maatschappelijk belang vanwege de bijzondere deskundigheid van het NFI en na verkregen goedkeuring van de minister van Justitie en Veiligheid.*

C. *het efficiënte, effectieve en veilige beheer van het hiermee gepaard gaande administratieve-, logistieke- en onderzoeksproces van stukken van overtuiging (SVO's) en andere zaken, vanaf de intake tot en met het opleveren van het onderzoeksrapport.*

D. *in het bijzonder de producten en diensten van de Divisies en Teams.*[12]

3.2 Grondslagen verwerken gewone persoonsgegevens

De grondslagen voor het verwerken van "gewone" gegevens zijn:
1. de verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang;
2. de verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting.[13]

3.2.1 Taak van algemeen belang

De Regeling taken NFI is een specifieke wettelijke uitwerking van een taak van algemeen belang.[14] [15] In het kader van die taken levert het NFI producten en diensten aan het Openbaar Ministerie, de

[12] In het register van verwerkingsactiviteiten is de verwerking opgesplitst naar het aandeel dat iedere Divisie en Team in de verwerking heeft. Hierbij worden de producten en diensten genoemd die in de SLA met het Openbaar Ministerie en de nationale Politie zijn vermeld. Hierdoor is het volstrekt transparant waarvoor het NFI persoonsgegevens verwerkt.
[13] Zie artikel 6, lid 1, sub c en d, AVG.
[14] Zie voor de kerntaken, de producten en diensten en de afnemers van de producten en diensten, de artikelen 1 t/m 3 van de Regeling van de minister van Veiligheid en Justitie, d.d. 8 mei 2012, nr. 227774, houdende bepalingen inzake de taakopdracht van het Nederlands Forensisch Instituut (Regeling taken NFI). De Regeling is ontleend aan de bevoegdheid van

Nationale Politie, de zittende magistratuur, de bijzondere opsporingsdiensten en het Ministerie van Justitie en Veiligheid.

De producten en diensten voor het Openbaar Ministerie en de Nationale Politie zijn (onder meer) benoemd in het Service Level Agreement (SLA) dat het NFI met het Openbaar Ministerie en de Nationale Politie is overeengekomen. Het leveren van producten en diensten door het NFI aan de Zittende Magistratuur, Bijzondere Opsporingsdiensten, zijn in die afspraken inbegrepen.[16] Het Openbaar Ministerie en de Nationale Politie hebben dit SLA ook namens hen geaccordeerd.[17] Op basis van dit SLA verkrijgt het NFI opdrachten van deze partijen, die zij weer op hun specifieke wettelijke bevoegdheden kunnen baseren.[18]

De Regeling taken NFI is via het Organisatiebesluit Ministerie van Justitie en Veiligheid, het Coördinatiebesluit organisatie en bedrijfsvoering rijksdienst 2011 terug te voeren op de Grondwet.[19]

De doelen van de verwerkingen en het type van de te verwerken persoonsgegevens door het NFI zijn inherent aan zijn kerntaken. Met de wettelijke grondslag voor de publieke taak is ook de wettelijke grondslag voor de verwerking van persoonsgegevens gegeven. Deze grondslag is voldoende precies.[20]

3.2.2 Wettelijke verplichting

Voor een verwerking op grond van een wettelijke verplichting geldt een noodzakelijkheidsvereiste: de verwerking moet noodzakelijk zijn om te voldoen aan de wettelijke verplichting. Deze wettelijke verplichting behoeft niet noodzakelijkerwijs te bestaan uit een expliciete verplichting om (bepaalde) persoonsgegevens te verwerken. Het komt namelijk ook voor dat de verwerking van persoonsgegevens een basis vindt in een wettelijke verplichting. In dit geval heeft de NFI een grotere eigen verantwoordelijkheid inzake het beoordelen van de noodzakelijkheid van de verwerking in het licht van het voldoen aan die wettelijke verplichting. Zonder verwerking van de

---

de minister op basis van art. 2, onder c, sub 5 en artikel 34 van de Organisatieregeling van het Ministerie van Veiligheid en Justitie. Deze Organisatieregeling is inmiddels vervangen door het Organisatiebesluit Ministerie van Justitie en Veiligheid 2017. De taakstelling van het NFI is verwoord in art. 42 van dit Organisatiebesluit. De Regeling taken NFI dient hier nog op te worden afgestemd. Zowel de voornoemde Organisatieregeling en het Organisatiebesluit zijn gebaseerd op artikel 3, lid 2 van het Coördinatiebesluit organisatie en bedrijfsvoering rijksdienst 2011. Dit Coördinatiebesluit is weer gebaseerd op art. 44, eerste lid, van de Grondwet. De Regeling taken NFI is hiermee een precieze wettelijke grondslag.

[15] Art. 6, lid 1, onder e, en lid 3, onder b, AVG.

[16] Service Level Agreement tussen het Nederlands Forensisch Instituut, de Nationale Politie en het Openbaar Ministerie, 21 december 2017. Zie ook de toelichting op de Regeling taken NFI, onder Algemeen en de artikelen 1, 2 en 4 (Strct 2012, nr. 9592, 18 mei 2012).

[17] Zie par. 19 SLA 2018.

[18] Zie o.a. de artikelen 150-151i;227-232 WvSv.

[19] Art. 44, eerste lid, van de Grondwet. Zie voor de kerntaken, de producten en diensten en de afnemers van de producten en diensten, de artikelen 1 t/m 3 van de Regeling van de minister van Veiligheid en Justitie, d.d. 8 mei 2012, nr. 227774, houdende bepalingen inzake de taakopdracht van het Nederlands Forensisch Instituut (Regeling taken NFI). De Regeling is ontleend aan de bevoegdheid van de minister op basis van art. 2, onder c, sub 5 en artikel 34 van de Organisatieregeling van het Ministerie van Veiligheid en Justitie. Deze Organisatieregeling is inmiddels vervangen door het Organisatiebesluit Ministerie van Justitie en Veiligheid 2017. De taakstelling van het NFI is verwoord in art. 42 van dit Organisatiebesluit. De Regeling taken NFI dient hier nog op te worden afgestemd. Zowel de voornoemde Organisatieregeling en het Organisatiebesluit zijn gebaseerd op artikel 3, lid 2 van het Coördinatiebesluit organisatie en bedrijfsvoering rijksdienst 2011. Dit Coördinatiebesluit is weer gebaseerd op art. 44, eerste lid, van de Grondwet.

[20] Zie MvT UAVG, pag. 29. Zie ook de opmerkingen van de Minister van Justitie over deze materie in het Advies Afdeling Raad van State en Nader Rapport, Tweede Kamer, vergaderjaar 2017–2018, 34 851, nr. 4, p. 33-39. Een en ander n.a.v. overweging 45 AVG en de betekenis hiervan voor de verwerkingspraktijk. Kort samengevat: Met een wettelijke grondslag voor een publieke taak of verplichting is niet steeds ook de wettelijke grondslag voor de gegevensverwerking gegeven. Dit is slechts het geval indien er sprake is van een voldoende precieze wettelijke grondslag.

gegevens moet het uitvoeren van een wettelijke verplichting redelijkerwijs niet goed mogelijk zijn.[21]

De verplichting voor het NFI om persoonsgegevens te verwerken kan in een voorkomende geval voortvloeien uit de Wet op de Deskundige in strafzaken (Wet DIS). Deskundigen van het NFI kunnen op grond van deze wet van de rechter-commissaris of het openbaar ministerie opdrachten krijgen voor het uitvoeren van een deskundigen onderzoek.[22] Binnen de bandbreedte van die opdracht kunnen de hiervoor geëigende persoonsgegevens worden verwerkt. Dit is inherent aan de verkregen opdracht.

Zoals in de voorgaande paragraaf reeds is opgemerkt, heeft de politie de bevoegdheid om aan het NFI technisch(opsporings)onderzoek op te dragen, waarvoor geen deskundigen benoeming vereist is. Deze bevoegdheid van de politie is afgeleid van de bevoegdheid van de officier van justitie en is gebaseerd op andere bepalingen in het Wetboek van Strafvordering.[23] In de aanwijzing Technisch onderzoek/deskundigenonderzoek is aangegeven voor welke onderzoeken wel en niet een benoeming als deskundige vereist is. Volgens deze Regeling sluit de Producten en Diensten Catalogus van het NFI hier nauw op aan.[24] In die zin kan het NFI onderscheid maken in te hanteren grondslagen voor het uitvoeren van opdrachten en hiermee gepaald gaande verwerkingen van persoonsgegevens. Soms ontstaat er in een zaak met meerdere opdrachten van diverse opdrachtgevers samenloop met wettelijke grondslagen.

Tenslotte zijn er verdragen, zoals het Verdrag van Prüm en het Internationale Rechtshulp Verdrag waaruit verplichtingen voortvloeien en die in specifieke gevallen als grondslag kunnen worden aangemerkt.

3.2.3 Opmaat naar bijzondere en strafrechtelijke gegevens

De voornoemde grondslagen zijn afhankelijk van de aan het NFI gegeven opdracht, ieder voor zich of gezamenlijk, de opmaat naar het verwerken van bijzondere en strafrechtelijke gegevens.
Het verwerken van bijzondere en strafrechtelijke persoonsgegevens is namelijk verboden, tenzij het NFI zich kan beroepen op:

a. een specifieke wettelijke uitzondering, én
b. tegelijkertijd één van de hiervoor genoemde grondslagen voor "gewone gegevens".

De specifieke uitzonderingen zijn uiteenlopend van rechtskarakter. Sommige uitzonderingen zijn rechtstreeks toepasselijk op basis van de AVG. Andere uitzonderingen moeten worden gevonden in Nederlands recht, Unierecht of verdragen. Dit kan in een (sector) specifieke wet, of in een van de meer regelingen voor afwijking van het verbod in de Uitvoeringswet AVG (UAVG).[25] Ten aanzien van de verwerkingspraktijk van het NFI kan worden gesproken van samenloop tussen de grondslagen en uitzonderingen voor gewone, bijzondere en strafrechtelijke gegevens. Met andere woorden: een grondslag voor gewone gegevens, kan tegelijkertijd als uitzondering gelden voor het verwerken van bijzondere en strafrechtelijke gegevens. Grondslagen en uitzonderingen worden

[21] Zie ook hier de opmerkingen bij noot 14.
[22] Een opdracht van de rechter, de RC, het openbaar ministerie en politie aan het NFI op grond van het Wetboek van Strafvordering (o.a. de artikelen 51i t/m 51m; 150 t/m 151i WvSv; 227 t/m 237). In de Memorie van Toelichting Wet DIS wordt diverse malen aan de deskundigen van het NFI gerefereerd. Ook de kerntaken van het NFI krijgen aandacht. Zie hiervoor MvT Wet DIS, Tweede Kamer, vergaderjaar 2006-2007, 31116, nr. 3, pag. 5, 7, 8 en 15.
[23] Zie MvT Wet DIS, pag. 10.
[24] Zie Aanwijzing technisch opsporingsonderzoek/deskundigenonderzoek, pag. 3, noot 4. In MijnNFI, de portal waartoe de politie toegang heeft, is per product of dienst vermeld of hiervoor een deskundigen benoeming, opdracht van de RC of OvJ, of toestemming van de OvJ nodig is.
[25] Zie MvT UAVG, p. 36.

hier als het ware "met elkaar verweven." Dit kan het gevolg zijn van het interdisciplinair door teams werken aan de uitvoering van een verkregen opdracht of zaak. Hieronder wordt verder ingegaan op de uitzonderingen voor bijzondere en strafrechtelijke gegevens.

3.2.3 Uitzonderingen voor bijzondere persoonsgegevens
Het NFI kan voor het verwerken van bijzondere gegevens een beroep doen op de volgende uitzondering in de AVG:

de verwerking is noodzakelijk om redenen van zwaar wegend algemeen belang, op grond van het Unierecht of Nederlands recht,
met als bijkomende voorwaarden:

- *waarborgen van de evenredigheid met het nagestreefde doel wordt gewaarborgd;*
- *wezenlijke eerbieding van de inhoud van het recht op bescherming van persoonsgegevens;*
- *treffen van passende en specifieke maatregelen ter bescherming van de grondrechten en de fundamentele belangen van de betrokkene.*

Vervolgens ontstaat er samenloop en gelaagdheid met:

- De Regeling taken NFI: bijzondere persoonsgegevens in samenhang met de SLA.

en afhankelijk van de ontvangen opdracht, met:

- De Wet DIS (bijzondere persoonsgegevens in samenhang met de SLA).
- Overige bepalingen van het Wetboek van Strafvordering waaraan het openbaar ministerie en de politie bevoegdheden voor opdrachten voor technisch (opsporings) onderzoek aan kunnen ontlenen.

Afhankelijk van de specifieke verwerkingssituatie kan naar keuze worden toegevoegd:

- De Wet DNA in strafzaken;
- De Regeling DNA in strafzaken;
- De Wet DNA-onderzoek bij veroordeelden;
- Besluit alcohol, drugs en geneesmiddelen in het verkeer;
- Verdragen, zoals het Verdrag van Prüm en Internationale Rechtshulpverdragen.

3.2.4 Uitzonderingen voor strafrechtelijke persoonsgegevens
Het NFI kan voor het verwerken van strafrechtelijke gegevens een beroep doen op de volgende uitzondering in de AVG:

> *het verwerken onder toezicht van de overheid of indien de verwerking is toegestaan bij Unierechtelijke of lidstaatrechtelijke bepalingen die passende waarborgen voor de rechten en vrijheden van de betrokkenen bieden.*[26]

Ook hier ontstaat samenloop en gelaagdheid met:

- De Regeling taken NFI (strafrechtelijke gegevens in samenhang met de SLA);
- De Wet DIS (strafrechtelijke gegevens in samenhang met de SLA).

Daaraan kunnen afhankelijk van de specifieke verwerkingssituatie naar keuze worden toegevoegd:

- De Wet DNA in strafzaken;
- De Regeling DNA in strafzaken;
- De Wet DNA-onderzoek bij veroordeelden;
- Besluit alcohol, drugs en geneesmiddelen in het verkeer;
- Verdragen, zoals het Verdrag van Prüm en Internationale Rechtshulpverdragen.

3.3 Toereikendheid grondslagen en uitzonderingen voor primaire verwerkingen

De hierboven vermelde grondslagen en uitzonderingen voor de primaire verwerkingen van het NFI zijn toereikend.[27] Tot dusver zijn er uit de inventarisatie van de verwerkingen geen aanwijzingen naar voren gekomen, die aanleiding geven voor twijfel.

3.4 Advies

Het gaat hier om een complexe juridische materie. Niet kan worden uitgesloten, dat in het natraject van de implementatie van de AVG inzichten op dit terrein worden herijkt.[28] Hierbij kan de behoefte ontstaan aan een specifieke en uniforme voorziening voor het verwerken van bijzondere en strafrechtelijke gegevens door het NFI. Dit kan bijvoorbeeld door een specifieke regeling toe te voegen aan de UAVG of een hierop te baseren algemene maatregel van bestuur. Of door de Regeling Taken NFI hiermee aan te vullen. Om die reden volgt hierbij het advies om de stellingname in deze memo tijdig door de wetgevingsjuristen van het Ministerie van Veiligheid en Justitie te laten toetsen.

---

[26] Zie art. 10 AVG.
[27] In deze memo worden de UAVG, de Wet politiegegevens (Wpg) en de Wet justitiële en strafvorderlijke gegevens (Wjsg) als grondslagen voor het verwerken van bijzondere en strafrechtelijke gegevens tot zover buiten beschouwing gelaten. Hierin zijn geen vooralsnog geen bruikbare grondslagen en uitzonderingen voor het NFI herkend.
[28] Een en ander bijvoorbeeld in vervolg op de discussie die zich n.a.v. overweging 45 AVG en de betekenis hiervan voordeed in het bij noot 14 en 15 aangehaalde Advies Afdeling Raad van State en Nader Rapport, Tweede Kamer, vergaderjaar 2017–2018, 34 851, nr. 4, p. 33-39.