5.

Nederlands Forensisch Instituut
Ministerie van Justitie en Veiligheid

10.2.e
Information Security Manager

10.2.e
Privacy Officer

Laan van Ypenburg 6
2497 GB Den Haag
Postbus 24044
2490 AA Den Haag
www.forensischinstituut.nl

Datum
3 juli 2020

Opgesteld door
10.2.e
sr. digitaal forensisch adviseur

Ons kenmerk
PIA Hansken advies
versie 1.0

nota

Managementreactie DBS op PIA's Hansken

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 separaat 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 gebruikt 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: middel

Het privacy statement op de NFI-website 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 voor het verbergen van geheimhoudersinformatie. Om (medewerkers van) organisaties die Hansken (willen) gebruiker 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 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: middel

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: middel

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: middel

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: middel

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: middel

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: middel

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: middel

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 toegang verlenen tot zaakdata op zowel de zakenservers als onderzoeks-omgevingen, waaronder Hansken (ontwikkel-, test-, experimenteer- en productie-omgevingen) en de onderzoekmachines en werkplekken van medewerkers.

Deze procedure moet tevens vastleggen hoe en wanneer de zakenservers 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 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) gebruiker hierover goed te informeren, moet voor Hansken een privacy-statement worden opgesteld en beschikbaar gesteld aan de gebruikers.

Advies is om het opstellen en beschikbaar stellen van dit statement op te nemen binnen het programma OK Hansken in de programmaopdracht '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 Hansken 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 statement kan hiervoor als input gebruik worden. Gewenste aanpassingen aan Hansken om maatregelen na te leven kunnen in overleg worden opgenomen binnen de programmaopdracht '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 programmaopdracht '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 bewaartermijnen zaakdata in Hansken	Automatische notificatie 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	Auditfunctie 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