Aanpassingen Hansken nav PIA

De Privacy Impact Assessment (PIA) is uitgevoerd voor de implementatie bij het NFI t.b.v. zaakspecifieke software-ontwikkeling (1A) of zaakonderzoek (1B).

Wat betreft noodzakelijke aanpassingen zijn de volgende drie types te onderscheiden:

- **NFI implementatie:** Specifiek voor de Hansken implementatie hier bij NFI (zowel 1A als 1B)
- **Software:** Noodzakelijke aanpassingen in de Hansken software, welke beschikbaar worden voor alle implementaties
- **Overig:** Aanpassingen in procedures en software die niet direct gerelateerd is tot Hansken (bijvoorbeeld de website van het NFI). Deze laatste categorie is hier niet meegenomen.

Deze pagina beschrijft de voorgenomen technische maatregelen in Hansken (aanpassingen aan de software) naar aanleiding van de PIA zaakonderzoek uitgevoerd met Hansken (varianten 1A en 1B) in 2019. Eventueel benodigde procedurele en organisatorische aanpassingen, en aanpassingen aan andere technische systemen zijn hier niet meegenomen.

PIA 1 Transparantie / rechten betrokkenen

Audit logging (software)

HBACKLOG-16 - **Hansken audit Logging** ACCEPTED

Als Security Officer / Eindgebruiker

Wil ik dat Hansken audit logging heeft

Zodat mogelijke wijzigingen verklaard kunnen worden en de CoE geborgd blijft (en zodat Hansken voldoet aan wet- en regelgeving)

PIA 2 Update privacy statement

Overige aanpassingen nodig (niet uitgewerkt)

PIA 3 Bewaartermijnen

Automatische waarschuwing slapende zaken (software)

Als Operator / Privacy Officer (welke?)

Wil ik een waarschuwing ontvangen wanneer een zaak een bepaalde periode (welke?) door niemand is ingezien

Zodat ik een aanleiding heb om te verifiëren of een zaak verwijderd kan worden

PIA 4 Toegang en autorisatie

Onderstaande drie user stories zouden goed gezien kunnen worden als NFI implementatie. De reden dat ze toch als software gelabeld zijn is dat bij Hansken ook autorisatie servers meegeleverd worden en iedere organisatie die deze gebruikt ook soortgelijke feedback van een PIA kan verwachten.

Audit aanpassingen autorisatie (software)

HBACKLOG-16 - **Hansken audit Logging** ACCEPTED

Als Privacy Officer

Wil ik in de audit trail kunnen terugzien wie wanneer welke aanpassingen in de autorisatie heeft gemaakt

Zodat ik weet wie wanneer toegang had tot zaakdata, wat zijn of haar rechten waren en wie hiervoor verantwoordelijk was

Beheerconsole zaaktoegang (software)

Als Zaak Operator

Wil ik in Hansken (of ergens anders?) kunnen beheren (inzien en aanpassen) wie welke autorisatie krijgt tot mijn zaak

Zodat ik overzicht heb wie er toegang heeft tot mijn zaak, en autorisaties gemakkelijk kan aanpassen indien nodig

Einddatum autorisatie (software)

Als (Zaak) Operator

Wil ik wanneer ik een autorisatie geef, hier een einddatum aan kunnen meegeven

Zodat ik kan voorkomen dat mensen te lang toegang blijven houden tot een zaak

PIA 5 Inperken bevoegdheden experimenteeromgeving

Misschien moeten de drie user stories hieronder herzien worden. Alternatief is het ontmantelen van de experimenteeromgeving op het moment dat externe ((nog) niet door het NFI geverifieerde) modules kunnen worden ingezet. De bedoeling is dat indien er operationele noodzaak is om zo snel mogelijk nieuwe extractie functionaliteit te kunnen uitproberen op productiedata, zonder dat productiedata gemodificeerd kan worden en met behoud van een volledige audittrail.

Auditlogging experimenteeromgeving (NFI implementatie)

Als Privacy Officer

Wil ik dat gebruikersacties in de experimenteeromgeving ook worden ge-audit

Zodat ik kan controleren of er geen gebruikers zijn die onrechtmatig zaakdata hebben ingezien

Autorisatie experimenteeromgeving tegen productieomgeving (NFI implementatie)

Als Privacy Officer

Wil ik dat gebruikers van de experimenteeromgeving geauthentiseerd worden tegen de autorisatie servers in productie

Zodat ik zeker weet dat alle procedures en controles die plaatsvinden in productie voor het verlenen van toegang tot zaakdata ook plaatsvinden bij het toegang verlenen tot de experimenteeromgeving

Expliciete toegang op *user added data* (software)

Als Zaak Operator

Wil ik toegang tot *user added data* kunnen ontzeggen aan iemand met toegang tot mijn zaak

Zodat ik kan voorkomen dat iemand uit de experimenteeromgeving toegang krijgt tot sporen die zijn toegevoegd door rechercheurs aan mijn zaak

PIA 6 Inrichten logging en monitoring op logging

Audit logging (software)

HBACKLOG-16 - Hansken audit Logging ACCEPTED

Er wordt gesproken over monitoring op de logging. Als dit betekent dat er een alarm moet afgaan op het moment dat auditlogging niet werkt dan is dit gedekt door voornoemde audit logging. Als dit een *audit the auditor* functie betreft dan is dit geen onderdeel van Hansken. Dit zal door de SIEM oplossing dit de audittrail beheert moeten worden aangeboden.

Ook automatische handhaving van de bewaartermijn voor de logs zal door de SIEM oplossing moeten worden aangeboden.

PIA 7 Screening

Overige aanpassingen nodig (niet uitgewerkt)

PIA 8 Beveiliging van uit Hansken geëxporteerde data

Voorkomen export GHC (software)

Als Geheimhoudingsmedewerker

Wil ik dat geheimhouderscommunicatie (GHC) alleen door geheimhoudingsmedewerkers kan worden geëxporteerd

Zodat wordt voorkomen dat GHC wordt ingezien door rechercheurs die op een zaak werken

Wat

Sporen die GHC bevatten mogen niet worden geëxporteerd, behalve door een Geheimhoudingsmedewerker. Dit houdt bijvoorbeeld in dat als een bestand met duizenden emails één GHC email bevat, dat dit hele bestand niet geëxporteerd kan worden door een rechercheur. Als informatie uit dit bestand toch geëxporteerd moet worden, moet dit door de Geheimhoudingsmedewerker worden gedaan die dan handmatig ervoor moet zorgen dat alleen de benodigde en toegestane sporen ter beschikking worden gesteld aan de rechercheur.

PIA 9 Datalekken

Overige aanpassingen nodig (niet uitgewerkt)

PIA 10 Verificatie adres van ontvanger

Overige aanpassingen nodig (niet uitgewerkt)

PIA 11 Opstellen verwerkersovereenkomst

Overige aanpassingen nodig (niet uitgewerkt)

PIA 12 Betrouwbaarheid

Borging testproces (software)

Als Hansken Product Owner / Product Manager

Wil ik dat aan de *Definition of Done* (de criteria waaraan een feature moet voldoen voordat deze als *klaar voor oplevering* wordt beschouwd) wordt toegevoegd dat voor elke nieuwe feature een representatieve test is geschreven die met succes wordt doorlopen

Zodat correcte werking van deze feature is geborgd

Testrapport (software)

Als Technisch Rechercheur

Wil ik indien nodig een testrapport kunnen overleggen in de rechtszaal

Zodat ik de correcte werking van Hansken aannemelijk kan maken.

NB: Voordat dit kan worden gedaan zijn er een aantal technische en infrastructurele aanpassingen nodig welke zijn opgenomen als kandidaat feature in het programma OK Hansken.

Certificatie van de Hansken programmatuur is niet mogelijk omdat deze gebruik maakt van componenten waarop geen invloed kan worden uitgeoefend zoals Hadoop en Elasticsearch.

PIA 13 Datakwaliteit

Controlegetallen images (software)

Als (Zaak) Operator

Wil ik dat Hansken controlegetallen of hashtotals berekend over geïmporteerde images vóórdat er gerapporteerd wordt

Zodat ik door middel van vergelijking met de aangeleverde controlegetallen kan vaststellen dat Hansken het image correct heeft ingelezen.

Deels door HBACKLOG-5 - Image Integrity CLOSED gerealiseerd.

PIA 14 Onrechtmatig datagebruik

Zie PIA 6 Inrichten logging en monitoring op logging