Privacy Impact Analyse

PRIVACY IMPACT ANALYSE

Toetsmodel Privacy Impact Assessment Rijksdienst (pdf)

I. Beschrijving van de gegevens

I.1. Welke gegevens

10.2.e :Hansken is een digitaal forensich systeem voor het onderzoek van digitale SVO's in een strafrechtelijk onderzoek en forensische research. Dit houdt in dat gegevens over godsdienst, levensovertuiging, ras, politieke gezindheid, gezondheid, seksueel leven, lidmaatschap van vakverenigingen en/of strafrechtelijk verleden onderwerp van het strafrechtelijk onderzoek kunnen zijn. Volgens de WBP (art 16) wordt dit omschreven als bijzonder gevoelige persoonsgegevens.

Volgens de in de beschrijving opgenomen criteria is het NFI zelf geen verantwoordelijke voor de verwerking. Immers, de data wordt ons aangeleverd door b.v. de politie of belastingdienst, waarna de data onder hun bevoegdheid verwerkt wordt. Echter, het is voor de verdere analyse wel een goede zaak om de gegevens te behandelen alsof het NFI de verantwoordelijke is voor de gegevens, wat voor het vervolg van deze analyse dan ook aangenomen wordt.

10.2.e : Ik ben het niet eens met de conclusie dat het NFI 'slechts" verwerker is. De "entiteit" die het doel van en de middelen voor de verwerking van persoonsgegevens vastlegt wordt aangemerkt als de verantwoordelijke. Dit is het NFI ! Zou dus onderwerp van gesprek moeten zijn tussen NFI en FG/CIO

10.2.e Daarnaast is het zo dat het niet om het NFI gaat maar om Hansken. Als Hansken bij de opdrachtgever staat, blijft de data en dus ook het resultaat van de analyse en de logs bij de opdrachtgever. Enige interessante is in dat geval dat het NFI graag (geanonimiseerde) logs ontvangt van de analyseresultaten.

In de data is twee typen gegevens te onderscheiden. Het eerste type gegevens (verder aangeduid met G1) bestaat uit 10.2.e : een forensische kopie van) alle gegevens die iemand zelf op zijn computer en/of telefoon en/of andere electronica heeft. De ervaringen van NFI-onderzoekers laten zien dat deze gegevens betrekking hebben op alle specifiek genoemde gegevens uit het Wbp. Het is echter niet op voorhand vast te stellen of dit type gegevens ook aanwezig is in de data die overgedragen worden 10.2.e Overgedragen aan wie?

Het tweede type gegevens (verder aangeduid met G2) zijn gegevens over de gebruikers van het systeem. 10.2.e : Data privacy (G1) en professional privacy (G2)

I.2.a. Andere specifieke gegevens

In G1 kunnen ook andere specifieke gegevens voorkomen, zoals die gegevens die informatie 10.2.e er de financiële of economische situatie van betrokkenen : of andere gegeven die kunnen leiden tot stigmatisering of uitsluiting)

10.2.e de tekst "sexuele geaardheid of religieuze situatie" weglaten omdat dit al bij de bijzonder gevoelige persoonsgegevens aan de orde is gekomen..

In G2 zullen geen gegevens voorkomen over financiele of economische situatie van betrokkenen.

I.2.b. Gevens over kwetsbare groepen

In G1 kunnen gegevens voorkomen over of van kwetsbare groepen, zoals minderjarigen, klokkenluiders, 10.2.e : mensen die te maken hebben met stalking of informanten voor politie of OM). tekst "of andere in de PIA genoemde groepen" weglaten.

In G2 zullen geen gegevens voorkomen over de in de genoemde groepen, met uitzondering mogelijk van informanten van politie of OM.
10.2.e en wat dan als we een (advocaat van een) verdachte of slachtoffer toegang geven i.v.m. b.v. schoning van geheimhoudersdata?

I.2.c. Gebruikersnamen en -wachtwoorden

In G1 kunnen (10.2.e zullen?) gebruikersnamen en -wachtwoorden voorkomen.

In G2 zullen gebruikersnamen en -wachtwoorden voorkomen.

I.2.d. Biometrische gegevens

Het is niet de bedoeling om biometrische gegevens in G1, noch in G2 op te nemen 10.2.e In G1 kunnen mogelijk biometrische gegevens voorkomen)

I.2.e. Verwerking BSN of andere persoonsgebonden nummers

In G1 kunnen andere persoonsgebonden nummers, waaronder telefoonnummers en IP-adressen, voorkomen.

In G2 zal hoogstens een telefoonnummer voorkomen.
10.2.e ook bijvoorbeeld "kledingnummers" van politiemedewerkers.

I.3. Uitleg bij de typen persoonsgegevens onder I.1 en I.2

Zonder de gegevens in G1 te verwerken en daarna ter beschikking te stellen van de aanvrager, kunnen geen (of minder) strafrechtelijke onderzoeken gebruik maken van data afkomstig van in beslag genomen gegevens 10.2.e Anders formuleren)

Zonder de gegevens in G2 is het niet mogelijk dat gebruikers gebruik maken van het systeem. De toevoeging van telefoonnummer is 'handig' ivm het contact opnemen met die betreffende gebruiker, maar niet strikt noodzakelijk.

10.2.e Voor forensische research worden de (bijzonder gevoelige) persoonsgegevens geanonimiseerd 10.2.e Alleen in de logs worden de gegevens geanonimiseerd

I.4. Anonimisatie of pseudonimisatie

Zaaksanalyse:
Voor de verwerking van de data in het kader van analyse van één zaak, kan alleen op de niet-geanonimiseerde voldoende resultaat gehaald worden. Dat staat niet tegen dat ook rekening gehouden wordt met geheimhouderscommunicatie (zie ook §III.4).

Nieuwe onderzoeksmethoden:
Voor de verwerking van de gegevens ten behoefte van het ontwikkelen van nieuwe onderzoeksmethoden 10.2.e n: bedoel je hier forensische research?) is het afdoende dat onderzoekers beschikken over de geanonymiseerde versie van de logbestanden 10.2.e : dus geen oorspronkelijke gegevens of data) die tijdens het verwerken van de data gecreerd worden. Indien het noodzakelijk is om de data zelf in te kijken, dient toestemming verkregen te worden van de dataowner (bijvoorbeeld de teamleider van de politie belast met het onderzoek).

Auditors:
Voor het uitvoeren van (gebruikers-)audits kunnen de auditors beschikken over de volledige niet-geanonimiseerde 10.2.e doel je hier niet juist de geanonimiseerde?) logbestanden - maar niet over de originele data. Indien het voor een auditor nodig is om te beschikken over de originele data, dient die bevoegdheid separaat verkregen te worden, hetzij via de data-owner, hetzij via het escrow-mechanisme 10.2.e Uitleggen wat je hier bedoeld).

I.5 Beleidsmatig kader

Ja.

10.2.e Hansken wordt ontwikkeld als technische opvolger van XIRAF. Er wordt dus gebruik gemaakt van nieuwe technologie binnen de reeds bestaande wettelijke en beleidskaders.

10.2.e moeten we hier ook niet aangeven welk kader het dan precies betreft? Iets met intelligence, opsporing en/of strafrecht?

II. Doelbinding

II.1 Doelbinding - specifieke doelen

10.2.e De rechtvaardiging voor het verwerken van bijzonder gevoelige persoonsgegevens in het kader van digitale forensische opsporing wordt gevonden in: ??? (opdrachtformulering/wetgeving voor het NFI? 10.2.e Taakopdracht: https://zoek.officielebekendmakingen.nl/stcrt-2012-9592.html

Deze vraag kan alleen gesteld worden aan de data-owner. @@ Niet juist: NFI is systeemeigenaar

10.2.e NFI is mogelijk niet ALTIJD systeemeigenaar van Hansken, maar slechts leverancier. Hierover is nog niets vastgelegd met mogelijke gebruikers.

De doelbinding waar in het ontwerp rekening mee itaaks gehouden, is die van individuele zaaksonderzoeken naar één of meerdere verdachten. Het is niet onmogelijk voor een gebruiker om buiten deze doelbinding te treden (bijvoorbeeld voor het opbouwen van inlichtingen over nog niet bekende verdachten voor andere delicten), maar het is niet mogelijk om dat te doen zonder een audit-trail.

II.2 Nieuwe of oude gegevens voor bestaand doel

Het systeem is geschikt om op een nieuwe en efficientere manier data te analyseren die reeds beschikbaar is, maar minder toegankelijk. Daarmee is het geen nieuw doel en geen nieuwe gegevens.

10.2.e Mogelijk worden wel nieuwe gegevens inzichtelijk doordat research nieuwe methoden oplevert die automatische nieuwe (sporen van) persoonsgegevens beschikbaar maken.

10.2.e Dit zijn dan geen nieuwe gegevens, maar bestaande gegevens die inzichtelijk worden gemaakt. Er ontstaan wel nieuwe gegevens doordat logbestanden op één locatie samen komen, waardoor andere analysemogelijkheden ontstaan (Bayest, trends, etc.). Bovendien gaat dit om G1. Voor G2 geldt dat ineens wel nieuwe gegevens worden verzameld die niet met EnCase of FTK worden verzameld, zoals een audit log.

II.3 Nieuw of uitbreiding systeem voor nieuw doel

Het systeem heeft geen uitbreiding van de doelbinding tot gevolg.

II.4 Melding

Niet van toepassing.

10.2.e Mogelijk dus wel van toepassing.

II.5 Controles

Niet van toepassing

10.2.e : Mogelijk dus wel van toepassing.

Ik stel voor dat we sowieso een gesprek met de FG aangaan (

~~HANSKEN-377~~ - Discussion Privacy Impact Assessment with Functionary Data Protection CLOSED). Hopelijk kan deze persoon ons helpen met deze afwegingen.

II.6 Kwaliteit

Voor G1 wordt na elke verwerking een analyse gedaan om de kwaliteit van de analyse vast te stellen.

10.2.e : Wat zegt de kwaliteit van de analyse over de juistheid/nauwkeurigheid/actualiteit van de persoonsgegevens? Of doet dat er niet toe?

De kwaliteit van de analyse bepaalt of de persoonsgegevens in de brongegevens correct worden gerepresenteerd. Of de persoonsgegevens in de brongegevens correct zijn valt buiten scope van het systeem.

Voor G2 wordt periodiek een audit gedaan om vast te stellen of de gegevens in de verzameling nog up-to-date zijn. Hierbij wordt uitgegaan van de laatste datum van gebruik van een individuele gebruiker.

10.2.e : De persoonsgegevens maken geen deel uit van Hansken zelf, maar van de omgeving waarbinnen Hansken benaderd wordt. Moeten we iets over roepen?

De persoonsgegevens die wij in logs opslaan, zoals username, IP-adressen, etc., zijn wel onderdeel van Hansken.

II.7 Profilering - gedrag

De gegevens uit G1 worden gebruikt om gedrag van personen vast te stellen.

De 10.2.e geanonimiseerde) gegevens uit G2 worden gebruikt om uit groepsgedrag efficientere wet af te leiden.

II.8 Profilering - geautomatiseerde analyse

Het systeem zal niet in staat zijn om op basis van de geautomatiseerde analyse op G1 of G2 autonoom vervolgacties te laten optreden (anders dan die acties die nodig zijn om de veiligheid van het gehele systeem en de opgeslagen data te waarborgen).

III.1 Betrokken instanties

- verwijzen naar het HLD en/of PAD.

III.2 Verantwoordelijkheid voor de bewerkingen

Tijdens elke fase van de verwerking is duidelijk welke partijen verantwoordelijk zijn voor de verwerking.

III.3 Beschikbaarheid van de informatie binnen de organisatie

...

III.4 Geheimhouderscommunicatie

Een deel van de data in G1 kan betrekking hebben op of afkomstig zijn van geheimhoudingsplichtigen. De verwerking daarvan wordt zo snel mogelijk gesignaleerd zodat het uitgesloten kan worden van verdere verwerking.

[Referentie toevoegen naar GHC-ontwerp]

III.5 In kaart brengen uitwisselingen

Ja, het is mogelijk om per data-owner aan te geven welke uitwisseling uitgevoerd kan worden.

III.6 Procedures voor creatie en wijzigingen

III.7 Uitwisseling met buitenland

Er wordt geen uitwisseling met het buitenland voorzien.

IV.1 Informatiebeveiligingsbeleid

Nog in te vullen.

IV.2 toezicht op bewerkers

Het toezicht op de bewerkers vindt plaats via een automatische en manuele analyse van acties die in het systeem uitgevoerd worden door die bewerker. Het systeem heeft daarnaast meerdere beveiligingsschillen die het zeer moeilijk maken voor een bewerker om over data te beschikken waar hij niet over hoort te beschikken.

IV.3 Beveiligingsmaatregelen

Nog in te vullen.
In ieder geval:
- bronbeveiliging
- Jericho
- CRAMM
- etc.

IV.4. Procedures in geval van inbreuk