



DPIA Security Monitoring

5.1.2.e

CBS Den Haag
Henri Faasdreef 312
2492 JP Den Haag
Postbus 24500
2490 HA Den Haag

5.1.2.e

www.cbs.nl

projectnummer

SSC
23 mei 2024

Inhoudsopgave

Inleiding	4
A. Beschrijving kenmerken gegevensverwerkingen	5
1.1 Verwerking van data t.b.v. de gegevensbescherming door middel van Security Monitoring	5
1.2 Geheimhouding	7
1.3 Persoonsgegevens	8
1.4 Gegevensverwerkingen	9
1.5 Verwerkingsdoeleinden	9
1.6 Betrokken partijen	9
1.7 Belangen bij de gegevensverwerking	10
1.8 Verwerkingslocaties	10
1.9 Techniek en methode van gegevensverwerking.	10
1.10 Juridisch en beleidsmatig kader	10
1.11 Bewaartermijnen	11
B. Beoordeling rechtmatigheid gegevensverwerkingen	13
2.1 Rechtsgrond	13
2.2 Bijzondere persoonsgegevens	14
2.3 Doelbinding	14
2.4 Noodzaak en evenredigheid	14
2.5 Rechten van de betrokkene	15
C. Beschrijving en beoordeling risico's voor de betrokkenen	16
3.1 Risico's	16
D. Beschrijving voorgenomen maatregelen	17
4.1 Uitwerking van de maatregelen	17
4.2 Maatregelen per risico	18

Inleiding

Dit is de gegevensbeschermingseffectbeoordeling (ook wel Privacy Impact Assessment genoemd, hierna: DPIA) van de security monitoring van het CBS.

Het CBS krijgt veel gegevens op basis van de Wet op het Centraal Bureau voor de Statistiek. Daarbij heeft het CBS de verantwoordelijkheid deze gegevens goed te beveiligen en heeft daarvoor security monitoring ingeregeld. Bij deze security monitoring wordt gebruik gemaakt van loggegevens die mogelijk gegevens bevatten over medewerkers van het CBS (hierna: de betrokkenen).

Deze DPIA is bedoeld als algemene DPIA voor security monitoring binnen het CBS.

A. Beschrijving kenmerken gegevensverwerkingen

In dit onderdeel wordt de voorgenomen gegevensverwerkingen, de verwerkingsdoeleinden en de belangen bij de gegevensverwerkingen uiteengezet.

1.1 Verwerking van data t.b.v. de gegevensbescherming door middel van Security Monitoring

Vanwege de taak waarmee het CBS belast is, worden er vele (bijzondere) persoonsgegevens binnen het CBS opgeslagen. Het is noodzakelijk om er op toe te zien dat deze gegevens op een adequate manier beschermd zijn tegen onrechtmatige bewerking, vervreemding of verwijdering. Hiervoor worden de logs van het infrastructuur- en applicatielandschap verzameld. Op basis van verwerking van en analyse van deze logs d.m.v. security monitoring, kan het CBS toezien dat de privacy- en gegevensbescherming op sommige aspecten gewaarborgd worden en levert inzicht op in mogelijke security-incidenten.

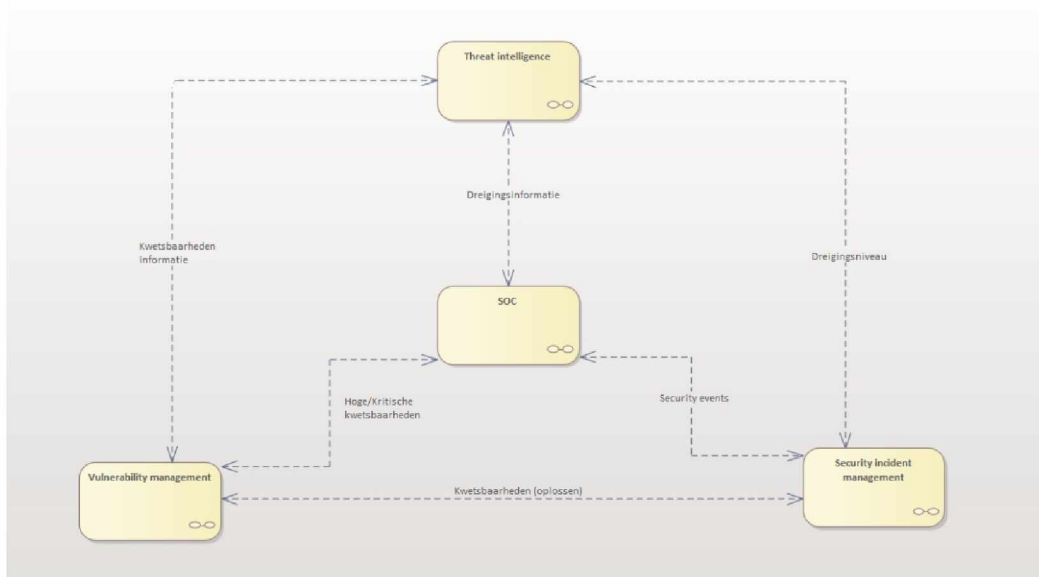
De scope van deze DPIA richt zich op de security monitoring van de IT-Infrastructuur, i.c. alle systemen, databases, applicaties en netwerkcomponenten, van het CBS. Onder de verwerking verstaan we het verzamelen, normaliseren, verrijken, aggregeren en correleren. Op basis hiervan worden vervolgens security-incidenten geïdentificeerd voor verdere incidentafhandeling conform geldende CBS praktijk in Topdesk.

1.1.1 Algemeen

Het CBS is een zelfstandig bestuursorgaan opgericht bij wet: de Wet op het Centraal bureau voor de statistiek (verder 'CBS-wet'). In het kader van de bewaking van de data (die het CBS voor de statistiek verwerkt), zodat deze niet onterecht buiten het CBS terechtkomt, verwerkt het CBS de logging van de infrastructuur en applicaties langs geautomatiseerde en handmatige weg.

Security monitoring houdt in, het monitoren van de IT-Infrastructuur, i.c. alle systemen, databases, applicaties en netwerkcomponenten, met als doel de bescherming van vertrouwelijke gegevens en het waarborgen van de integriteit, vertrouwelijkheid en beschikbaarheid van informatie. Door een gedegen security monitoring kan de organisatie hackpogingen door kwaadwillenden voorkomen en tijdig ingrijpen bij security incidenten, waardoor de beveiligingsrisico's sterk kunnen worden verminderd.

De security monitoring wordt continu in real-time uitgevoerd door het Security Operations Center-team (SOC) van het SSC met behulp van verschillende tooling/platformen. Het voornaamste platform betreft hierbij het SIEM/logplatform. In dit platform wordt de logging verzameld die voor de security monitoring van belang is.



Deze procesplaat beschrijft de drie kernprocessen (Vulnerability management, Threat Intelligence, Security incident management) en de daarin terug te vinden sub-processen die bijdragen aan het kernproces.

Vulnerability management is het proces van het identificeren, beoordelen en behandelen van kwetsbaarheden in computersystemen, netwerken, software, en andere IT-infrastructuur.

Threat intelligence houdt in het verzamelen van informatie over potentiële dreigingen en risico's om deze informatie te gebruiken bij het aanscherpen van de monitoring en beveiliging.

Security Incident Management (beveiligingsincidentbeheer) is het proces van het effectief reageren op en het beheren van beveiligingsincidenten die zich voordoen.

1.1.2 Taak:

Zie 1.1.1.

1.1.3 Uitvoeren (grondslag):

Voor het kunnen bewaken van gegevens is het noodzakelijk om security monitoring uit te voeren op de IT-infrastructuur van het CBS. Er ligt verdere onderbouwing voor het opslaan verzamelen en analyseren van logging in de BIO 2.0 norm 8.15 en 8.16. Ook adviseert het NCSC overheidspartijen de opgestelde richtlijnen te volgen. Hierbij vormen de richtlijnen voor loginformatie¹ en detectie verdere grondslag² tot het inrichten van security monitoring. De juridische grondslag is verder verwerkt in onderdeel B van de DPIA hierin wordt ook in gegaan op artikel 6 lid 1 sub f AVG.

¹ <https://www.ncsc.nl/onderwerpen/loginformatie>

² <https://www.ncsc.nl/onderwerpen/detectie>

1.1.4 Gebruik van de gegevens (doelbinding):

De gegevens worden verzameld in het kader van de security monitoring en analyse van de CBS omgeving op security incidenten. Het doel van deze gegevens is om de data die het CBS in beheer heeft, op een adequate manier te beveiligen en de processen soepel te laten lopen.

1.1.5 Toegang tot de data

De toegang tot de gegevens verwerkt door security monitoring is alleen mogelijk voor degenen die belast zijn met de verzameling, analyse en monitoring van de omgeving van het CBS en die in dat kader noodzakelijkerwijs toegang moeten hebben tot de betreffende data. Het combineren en correleren van verschillende log-sources voor monitoringdoeleinden is alleen toegestaan voor medewerkers van team SOC van het SSC.

De toegang tot de data is gescheiden d.m.v. Roll Based Access (RBAC) welke in het loggings en monitoringsplatform aanwezig is. Met behulp van de RBAC functionaliteit wordt de toegang tot specifieke velden afgeschermd zodat de medewerkers van het SOC alleen de informatie kunnen inzien die ze op basis van hun rol nodig hebben.

Tevens is het voor betrokken mogelijk om de gegevens die over hen worden verzameld in te zien. Dit gebeurt op aanvraag zoals beschreven onder paragraaf 2.5 van deze DPIA.

1.2 Geheimhouding

De logging die als input gebruikt wordt voor de security monitoring wordt centraal verzameld en vervolgens via RBAC toegankelijk gemaakt voor de SOC-medewerkers. Alleen SOC-medewerkers hebben toegang tot het totaal overzicht van deze logging.evens heeft de security monitoring-tooling de mogelijkheid tot data-masking en het pseudonimiseren van data. Additioneel zijn maatregelen getroffen zoals beschreven in paragraaf 4.1 van de DPIA.

1.2.1 Beveiliging

Om dataprivacy te waarborgen bij het uitvoeren van security monitoring, dient het aantal personen met toegang tot de logging beperkt te worden en dient het vier ogen principe te worden toegepast.evens zal men alleen relevante informatie verwerken bij het uitvoeren van security monitoring. Niet relevante informatie die uit de informatiebronnen komt, mag niet worden opgenomen in de tooling.

Om de kans op geautomatiseerde besluitvorming, profilering en ongeoorloofd monitoren verder te mitigeren, dient “monitoring op de monitoring” te worden uitgevoerd. Deze controle op de logs van SOC-medewerkers, zoals toegang tot monitoringsdata, dient te worden gebruikt om te beoordelen of de actie van de SOC-medewerker geoorloofd was. De eindverantwoordelijke van het SSC dient er op toe te zien, dat er geen ongebruikelijke patronen optreden, zoals oneigenlijk gebruik van rechten en/of gegevens. Ook dienen de gebruikte usecases periodiek te worden geëvalueerd. Indien medewerkers die security monitoring uitvoeren worden verdacht van misbruik, dient hun toegang tot data onverwijld geblokkeerd te worden en dient een onderzoek ingesteld te worden. Zo nodig kan voor dat onderzoek de hulp van een extern onderzoeksbureau worden ingeroepen.

1.2.2 Toetsing

Het CBS laat zich jaarlijks extern toetsen op de informatiebeveiliging (ISO 27001), kwaliteit (ISO 9001) en de privacybescherming (Privacy Control Framework van NOREA). De certificaten worden op de website van CBS gezet³.

³ <https://www.cbs.nl/nl-nl/over-ons/organisatie/privacy/iso-en-privacycertificering>

1.3 Persoonsgegevens

Bij security monitoring worden persoonsgegevens in de zin van de AVG verwerkt van betrokkenen. Er worden geen bijzondere persoonsgegevens verwerkt.

1.3.1 Diversiteit aan gegevens:

Bij het uitvoeren van security monitoring worden de volgende gegevens verwerkt, die uiteindelijk herleidbaar zijn tot individuele medewerkers van het CBS (betrokkenen):

- Inlogpogingen en gebruik van gebruikersaccounts
- IP-adressen van in en uitgaande netwerkverbindingen
- Activiteiten op systemen en applicaties, inclusief toegangs- en wijzigingspogingen
- Metadata van communicatie zoals tijdstempels, duur van verbindingen, e-mailadressen, bijlage naam en omvang van het bestand
- Inlogpogingen en gebruik van toegangspassen
- Locatie van apparaten (indien beschikbaar)

Het betreft de volgende mogelijke persoonsgegevens van de CBS werknemers die in de logging terecht komen tijdens het uitvoeren van hun gebruikelijke taken binnen het CBS:

- PID
- Gebruikersnaam
- E-mailadres
- IP-adres
- Systeemnaam
- DNS-naam (alias)

Er bestaat verder verschil tussen wat in de logs files wordt aangeleverd en door het platform wordt opgeslagen. De inhoud van de logging van de infrastructuur en het applicatie landschap wordt bepaald door de leverancier of developer(s) van de applicatie. Daardoor hebben wij in het platform geen invloed op welke informatie aangeleverd wordt. Voor elk platform dat gebruikt wordt voor security monitoring, dient vastgelegd te worden wat de benodigde⁴ velden voor het platform zijn. Vanwege BIO 2.0 norm 5.28 dient er een kopie van de log op de backup server te worden opgeslagen, hierbij dienen de standaard bewaartermijnen in achtgenomen te worden.

⁴ Deze velden zijn uitgewerkt in het bestand "logging-en-monitorings-velden.xlsx" welke in het volgende paragraaf verder uiteen wordt gezet.

1.4 Gegevensverwerkingen

Tijdens het onboardingsproces voor nieuwe security monitoring diensten, dienen nieuwe logsources te worden beoordeeld of deze logsource additionele velden bevat naast de velden vastgelegd in het document “logging-en-monitorings-velden.xlsx”. In dit document zijn de velden opgenomen die standaard opgenomen worden per log source type. Voor de volledigheid zijn hierin ook de persoonlijke identificeerbare velden opgenomen uit de vorige paragraaf.

In dit document is ook onderscheid gemaakt tussen velden die altijd aanwezig dienen te zijn in de log en velden die optioneel zijn. Op basis hiervan wordt vervolgens beoordeeld of er een DPIA voor de additionele velden noodzakelijk is. In deze additionele DPIA zullen eventuele additionele maatregelen vastgelegd worden voor deze nieuwe velden.

Een voorbeeld van dit overzicht is hieronder opgenomen ter verduidelijking:

Veld	Category	Wanneer vereist	Direct persoonlijk identificeerbaar	Indien beschikbaar	Waarom (typering uitgelegd in apart tabblad)	Wie heeft er toegang
Datetime	Generiek	Altijd	Nee	NVT	A, B, C	SSC & Dienst verantwoordelijke
IP (Source)	Generiek	Altijd	Ja	NVT	A, B, C	SSC & Dienst verantwoordelijke
IP (Destination)	Generiek	Altijd	Ja	NVT	A, B, C	SSC & Dienst verantwoordelijke
Port (Source)	Generiek	Altijd	Nee	NVT	A, B, C	SSC & Dienst verantwoordelijke

Aanpassing van het document “logging-en-monitorings-velden.xlsx” wordt altijd gecommuniceerd naar CPO, FG en mogelijk OR en geaccordeerd buiten BIM.

Na het verzamelen⁵ van de logging volgt het indexeren, analyseren en monitoren op afwijkingen en tot slot bewaren. Deze verwerkingen zijn vastgelegd in het register van de verwerkingsactiviteiten voor de desbetreffende security monitoring-dienst. Dit register is terug te vinden onder de naam SIEM-verwerkingsregister.xlsx. In het CBS-breed verwerkingenregister dient een verwijzing naar dit SIEM-verwerkingsregister opgenomen te worden.

1.5 Verwerkingsdoeleinden

Zie 1.1.4.

1.6 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 welke functionarissen binnen de organisaties toegang krijgen tot welke persoonsgegevens.

1.6.1 CBS (algemeen)

Het CBS is de enige partij welke data verwerkt binnen het systeem.

⁵ Het proces is beschreven in paragraaf 1.1.1 van dit document.

1.6.2 CBS (de organisatie)

Het CBS (de organisatie) heeft op de grond van de wetgeving rondom gegevensbescherming de rol als verwerkingsverantwoordelijke. De organisatie heeft de eindverantwoordelijkheid voor deze gegevensverwerking bij de CIO belegd. De CIO heeft de verantwoordelijkheid voor beleid rondom security monitoring aan de CISO gedelegeerd. De CISO rapporteert hierover terug aan de CIO.

1.6.3 SOC

De CIO heeft de taak rondom het monitoren op eventuele security incidenten gedelegeerd aan Hoofd SSC, en via Hoofd SSC aan het SOC-team van het Security Service Center, onderdeel van CBS IT afdeling BIT. Het SOC-team is verantwoordelijk voor het uitvoeren van de taak. Hoofd SSC is eindverantwoordelijk.

Het combineren en correleren van verschillende log-sources voor monitoringdoeleinden is alleen toegestaan voor medewerkers van het SOC. Alleen SOC-medewerkers hebben toegang tot het totaaloverzicht van de verschillende log-sources binnen het CBS.

1.7 Belangen bij de gegevensverwerking

De verwerking wordt uitgevoerd in het belang van 18 miljoen betrokkenen (burgers), zo'n 2 miljoen bedrijven waarvan gegevens worden verwerkt en de medewerkers van het CBS zelf, van wie allemaal gegevens worden verwerkt binnen het CBS. Al deze gegevens dienen adequaat beschermd te worden.

1.8 Verwerkingslocaties

De verwerkingslocatie is CBS in Nederland (Den Haag, Heerlen). Het datacenter is gevestigd in Almere. In Oudermeer is er een backup-, uitwijk- en storage uitwijklocatie gevestigd. Ook worden er gegevens extern in de cloud verwerkt, waarbij de locatie beperkt is tot de Europese Unie.

De overzeese vestigingen van het CBS vallen op dit moment buiten de scope van deze werking. Mogelijk wijzigt dit in de toekomst. Wanneer dat plaatsvindt zal de DPIA ook herzien worden.

1.9 Techniek en methode van gegevensverwerking.

De security monitoring-tooling maakt gebruik van machine learning en AI⁶ om events uit de verzamelde logs te correleren en waar nodig te alarmeren op mogelijke technische, security of privacy incidenten. Deze alarmering gebeurt automatisch op basis van voorgeprogrammeerde regels, "use cases", die bepaalde signalen of patronen herkennen in de logs en een alarm afgeven.

Technieken en methodes met automatische besluitvorming met aanzienlijke gevolgen voor betrokkenen, zoals rechtsgevolgen, zijn verboden. Profilerings dient niet toegepast te worden bij het maken van use cases in de security monitoring-tooling.

1.10 Juridisch en beleidsmatig kader

CBS-wet (02-03-2022), AVG (01-07-2021), BIO 2.0 verdere beschrijving in onderdeel B van deze DPIA.

⁶ Het betreft hier de machine learning en AI modellen zoals aangeleverd in het SIEM product.

1.11 Bewaartermijnen

In de Algemene verordening gegevensbescherming (AVG) staat geen concrete bewaartermijn voor persoonsgegevens. Organisaties bepalen zelf hoe lang zij persoonsgegevens bewaren. Het uitgangspunt is dat gegevens zo kort mogelijk worden bewaard. Hieronder worden de specifieke bewaartermijnen uiteengezet opvolgend van verplicht naar vrijblijvend.

1.11.1 Bewaartermijnen volgens BIO 2.0 norm

De logging waar security monitoring gebruik van maakt, dient minimaal een half jaar beschikbaar te zijn voor onderzoek. In geval van een (vermoedelijk) informatiebeveiligingsincident is de bewaartermijn van de gelogde incidentinformatie minimaal drie jaar. Bewaartermijnen van een log zijn onder andere beschreven in het BIO- product “Handreiking Dataclassificatie”⁷. Deze is uitgesplitst op basis van de verschillende eisen voor integriteit en vertrouwelijkheid. Hieronder een samenvatting van de bewaartermijnen, met in VET gedrukt de standaard volgens de BIO norm. Deze BIO norm zal door het CBS gehanteerd worden tenzij specifiek heroverwogen in de DPIA van een bepaalde logsource:

Integriteit

Niveau	Monitoring
Niet zeker	Geen
Beschermd	Vastleggen authenticatie (correct en foutief) en tijdstip. Vastleggen relevante input en output van een ICT-systeem of -service. Monitoring-gegevens bewaren voor periode van een half jaar.
Hoog	Vastleggen authenticatie (correct en foutief) en tijdstip. Vastleggen relevante input en output van een ICT-systeem of -service. Monitoring-gegevens bewaren voor periode van maximaal twee jaar of langer bij een vermoed beveiligingsincident.
Absoluut	Vastleggen authenticatie (correct en foutief) en tijdstip. Vastleggen relevante input en output van een ICT-systeem of -service. Monitoring-gegevens bewaren voor periode van minimaal drie jaar bij een vermeend beveiligingsincident. Vastleggen oude staat van te wijzigen gegevens.

Vertrouwelijkheid

Niveau	Monitoring
Openbaar	Geen
Bedrijfs- vertrouwelijk	Vastleggen herhaaldelijk foutieve authenticatie en tijdstip. Monitoring-gegevens bewaren voor periode van een half jaar.
Vertrouwelijk	Vastleggen herhaaldelijk foutieve authenticatie en tijdstip. Monitoring-gegevens bewaren voor periode van twee jaar.
Geheim	Vastleggen correcte en foutieve authenticatie en tijdstip. Monitoring-gegevens bewaren voor periode van zeven jaar.

Tabel 2: Bewaartermijn logging

1.11.2 Bewaartermijn CBS

⁷ <https://www.informatiebeveiligingsdienst.nl/product/handreiking-dataclassificatie-2/>

De beschikbaarheid van loginformatie, waar security monitoring van afhankelijk is, moet conform de BIO zijn gewaarborgd binnen de termijn waarin loganalyse noodzakelijk wordt geacht, met een minimum van drie maanden. De termijn waarin de mogelijkheid tot analyse van de loggegevens noodzakelijk moet worden geacht, is door de Taskforce BID gekoppeld aan de classificatie van de gegevens. Deze classificatie is nog niet afgerond waardoor het koppelen van de bewaartermijnen aan deze classificatie nog niet mogelijk is.

Binnen het CBS worden daarom de volgende hoofdlijnen gevolgd:

- Bij het standaard niveau van de BIO (departementaal vertrouwelijk, CBP risicoklasse II), dat ook voor CBS van toepassing is, geldt daarbij een bewaar termijn van maximaal 2 jaar.
- Bij een (vermoedelijk) beveiligingsincident geldt een minimum termijn van 3 jaar⁸.
- Voor openbare gegevens, zoals in StatLine en op de CBS website, kan het minimum termijn van 6 maanden worden aangehouden.

Indien verder specificatie noodzakelijk is dan wordt dit vastgelegd in DPIA van de specifieke logsource.

1.11.3 Bewaartermijn CBS backups

Het bewaartermijn voor de back-ups is 4 weken volgens de intranet pagina over de CBS backups⁹.

⁸ Op basis van BIO norm 5.28

⁹ <https://cbsintranet/pdc/Paginas/Backup.aspx>

B. Beoordeling rechtmatigheid gegevensverwerkingen

Op basis van de feiten zoals vastgesteld in onderdeel A wordt in dit onderdeel beoordeeld of de voorgenomen gegevensverwerkingen rechtmatig zijn. Het betreft hier de beoordeling van de juridische rechtsgrond, noodzaak en doelbinding van de gegevensverwerkingen. Ook wordt er aandacht besteed aan de rechten van de betrokkenen.

2.1 Rechtsgrond

Het CBS krijgt vanuit de wettelijke taak een grote hoeveelheid data van overheidsinstanties, burgers en bedrijven (**artikel 3 CBS-wet**) en is verantwoordelijk voor de beveiliging van zijn gegevens tegen verlies of aantasting en tegen onbevoegde kennisneming, wijziging en verstrekking van die gegevens (**artikel 38 CBS-wet**). Om hieraan te voldoen wil het CBS op een veilige en adequate manier monitoren of de data die het CBS ontvangt op een juiste manier gebruikt en beschermd wordt. Daarvoor is security monitoring noodzakelijk. De grondslag van deze security monitoring is **artikel 6, lid 1, onder e** (noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag). Dit slaat op artikel 38 van de CBS wet.

2.1.1 Additionele kaders:

Naast de grondslag dient het CBS en haar werknemers te voldoen aan de ambtenarenwet en de arbeidsovereenkomst. Onderstaand is gespecificeerd in welke vorm deze additionele kaders van toepassing zijn op security monitoring.

Artikel 3 CBS-wet:

Het CBS heeft tot taak het van overheidswege verrichten van statistisch onderzoek ten behoeve van praktijk, beleid en wetenschap en het openbaar maken van de op grond van zodanig onderzoek samengestelde statistieken.

Artikel 38 CBS-wet:

De directeur-generaal draagt op de voet van de ter zake voor de Rijksdienst geldende voorschriften zorg voor de nodige technische en organisatorische voorzieningen ter beveiliging van zijn gegevens tegen verlies of aantasting en tegen onbevoegde kennisneming, wijziging en verstrekking van die gegevens.

Uit de BIO-norm:

Norm 8.15, 8.16 en 5.28:

In deze norm worden kaders gesteld aan op welke manier een organisatie moet voldoen aan verslaglegging en monitoren. De doelstelling hier is het op een juiste manier vastleggen van gebeurtenissen (Bio 2.0-norm 8.15 en 8.16) en verzamelen bewijs (Bio 2.0-norm 5.28). De BIO norm is CBS breed van toepassing en hierdoor ook voor security monitoring.

Uit de Ambtenarenwet:

Artikel 9:

De ambtenaar en de gewezen ambtenaar zijn verplicht tot geheimhouding van hetgeen hen in verband met hun functie ter kennis is gekomen, voor zover die verplichting uit de aard der zaak volgt.

Uit de AVG:

Met betrekking tot artikel 6 lid 1 sub b AVG (arbeidsovereenkomst)

Medewerkers van het CBS tekenen een arbeidsovereenkomst bij indiensttreding. Onderdeel van deze arbeidsovereenkomst is een geheimhoudingsverklaring. Medewerkers verklaren hiermee dat alle vertrouwelijke informatie die uit hoofde van hun dienstverband aan hen bekend wordt, geheim zullen houden. Om te controleren of medewerkers zich ook daadwerkelijk houden aan deze geheimhoudingsverplichting, dient te worden gemonitord welke informatie, wanneer het CBS verlaat. Door ondertekening van de arbeidsovereenkomst verbindt een medewerker zich aan de Ambtenarenwet 2017, maar ook aan de CBS-wet.

Ten aanzien van Overige gegevens – niet zijnde statistisch o.b.v. CBS-wet:

Buitenom de bovenstaande verplichting geldt er, conform artikel 9 Ambtenarenwet 2017, een geheimhoudingsplicht voor werknemers binnen het CBS. Verder tekenen medewerkers bij indiensttreding bij het CBS een geheimhoudingsverklaring. Om te controleren of deze plicht wordt nagekomen door de medewerkers dient het CBS te kunnen inzien wat voor soort communicatie/informatie zij buiten het CBS brengen.

2.2 Bijzondere persoonsgegevens

De data die verzameld wordt door middel van security monitoring kan gevoelige informatie bevatten. Deze data kan de volgende informatie bevatten: bijzondere persoonsgegevens en microdata uit het statistisch proces. Verder is het noodzakelijk dat voor elke tooling die gebruikt wordt voor security monitoring een specificatie van welke data en velden opgeslagen worden. Dit dient verder uitgewerkt te worden in een DPIA van de desbetreffende tool.

2.3 Doelbinding

Security Monitoring op basis van verzamelde logging dient alleen het doel om de gegevens van de (onder 1.7 benoemde) betrokkenen te beschermen en van dit doel mag niet afgeweken worden. Dit betekent dat de verzamelde gegevens nergens anders voor gebruikt mogen worden dan voor dit doel.

Lange termijn opslag van verzamelde gegevens dient het doel om consistent en doeltreffend beheer van bewijsmateriaal te bewerkstelligen, in verband met informatiebeveiligingsincidenten. Verder kunnen er historische- en trendanalyse gemaakt worden op basis van de verwerkte gegevens binnen de kaders van de bewaartermijnen.

2.4 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?

Het is van groot maatschappelijk belang dat goed, deugdelijk (en voor zover nodig buiten de wettelijke taak uit artikel 38 CBS wet) wordt gecontroleerd welke gegevens het CBS verlaten en of daar geen vertrouwelijke informatie tussen zit. Ook is het van belang dat de gegevens niet ongeoorloofd geraadpleegd, gecombineerd of aangetast wordt. Dit maatschappelijke belang is groter dan het individuele belang van de medewerker.

b. Subsidiariteit: kunnen de verwerkingsdoeleinden in redelijkheid niet op een andere, voor de betrokkene minder nadelige wijze, worden verwezenlijkt?

Persoonsgegevens dienen zoveel mogelijk afgeschermd te worden binnen security monitoring. Echter bij analyses in meer detail kan zoals eerder opgemerkt niet voorkomen worden dat

medewerkers geïdentificeerd worden. Het beschermen van gegevens kan wellicht wel op een andere manier gehaald worden (bijvoorbeeld naast iedere medewerker twee controleurs die meekijken), maar niet op een minder ingrijpende wijze voor de betrokkenen. De AVG verplicht dat voor ingebruikname van elke nieuwe security monitoring tooling, een DPIA wordt uitgevoerd.

2.5 Rechten van de betrokkene

De betrokkenen in het kader van de DPIA zijn in eerste instantie de CBS werknemers. In het kader van security monitoring, kennen de betrokkenen de volgende rechten m.b.t. de data van de desbetreffende betrokkene:

- Recht op inzage van de gegevens
- Recht op rectificatie van de gegevens
- Recht op wissen van gegevens
- Recht op kennisgeving van rectificatie en wissen van gegevens.
- Recht op bezwaar
- Recht op beperking van verwerking
- Recht op overdraagbaarheid

In principe weegt het belang van de bescherming van data van burgers, bedrijven/overheidsinstanties en de rest van de CBS-medewerkers zwaarder dan dat van een individuele medewerker. Echter, in het geval van onjuist handelen bij potentiële incidenten, op basis van security monitoring, kan de medewerker aanspraak maken op bovengenoemde rechten. Dit geldt ook in het geval van onjuiste configuratie en werking van de security monitoring-tooling.

Voor deze rechten dienen de procedures vooraf aan de implementatie van nieuwe security monitoring tooling opgesteld te zijn. Op dit moment is het voorstel voor alle nieuwe diensten, om deze procedures op een gezamenlijk plek op te slaan zoals een werkruimte waarop de procedures en processen met eventuele verdere informatie is terug te vinden.

C. Beschrijving en beoordeling risico's voor de betrokkenen

In dit onderdeel worden de risico's van de voorgenomen gegevensverwerkingen voor de rechten en vrijheden van de betrokkenen uiteengezet. Hierbij worden de aard, omvang, context en doelen van de gegevensverwerking zoals in onderdeel A en B zijn beschreven meegenomen. De betrokkenen in deze zijn de medewerkers van het CBS.

3.1 Risico's

Onderstaand zijn de risico's voor betrokkenen uiteengezet die vastgesteld zijn ten aanzien van security monitoring.

1. Verwerkingsproces:
 - a. Systemen worden onnodig opgenomen in security monitoring producten, waardoor tijdelijk persoonsgegevens onnodig verwerkt worden gezien het doel van de verwerking.
 - b. Transparantie over (wijzigingen aan) de use cases is onvoldoende, waardoor CPO, FG en betrokkenen geen inzicht hebben in de verwerking van persoonsgegevens.
2. Security monitoring-proces:
 - a. Een medewerker van team SOC binnen het SSC heeft inzicht in de inhoud van logging die mogelijk (bijzondere) persoonsgegevens over CBS-ers bevat, en gebruikt deze onjuist, wat kan leiden tot potentieel misbruik door de medewerker van het SOC, met mogelijke consequenties voor de betrokkenen.
 - b. Het systeem genereert foute signalen (false-positives), waarop mogelijk onterecht geacteerd wordt door een medewerker van het SOC, met gevolgen voor CBS-ers/betrokkenen.
 - c. Medewerkers van het SOC, stellen usecases op, die betrokkenen vergaand profileren
 - d. Personeel van een leverancier van security monitoring-tooling in de cloud zouden toegang kunnen hebben tot de gegevens van betrokkenen
3. Afhandeling van incidenten:
 - a. Betrokkenen worden onterecht aangesproken;
 - b. Betrokkenen worden op onjuiste wijze aangesproken;
 - c. Betrokkenen worden door de verkeerde persoon aangesproken.
4. Opslag en transport van data:
 - a. Data wordt op een onveilige manier opgeslagen en getransporteerd, waardoor gegevens van betrokkenen onterecht zichtbaar is.
5. Misbruik van permissies:
 - a. Een medewerker van het SOC misbruikt de aan hem/haar toegekende permissies voor het inzien van (bijzondere) persoonsgegevens, buiten de gegevens die hij/zij nodig heeft voor de werkzaamheden binnen het SOC.

D. Beschrijving voorgenomen maatregelen

In onderdeel D wordt gezien 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 DPIA is, als het gaat om beveiligingsmaatregelen, expertise over informatiebeveiliging belangrijk.

4.1 Uitwerking van de maatregelen

4.1.1 Algemeen

Op basis van de CBS-brede risicoanalyse uit 2015 wordt geconcludeerd dat het CBS als organisatie op grond van de criteria die in de VIR-BI 2013 zijn genoemd het vertrouwelijkheidsniveau Departementaal Vertrouwelijk (Dep.V.) heeft. Tevens valt de verwerking van bijzondere persoonsgegevens onder risicoklasse 2 van de Autoriteit Persoonsgegevens.

Voor het vaststellen van de noodzakelijke maatregelen hanteert het CBS de ISO 27001/2 norm en de Baseline Informatiebeveiliging Overheid (BIO) 2.0 als uitgangspunt. Met de daaruit voorkomende maatregelen zijn de risico's voldoende afgedekt. Volledige afdekking van de risico's zal nooit mogelijk zijn omdat de menselijke factor, veelal de belangrijkste factor bij een beveiligingsincident, nooit volledig uit te sluiten is.

4.1.2 Scope

De scope van deze maatregelen omvat alle primaire en alle ondersteunende processen van het Centraal Bureau voor de Statistiek en de daarvoor gebruikte informatiesystemen, waarbij onder informatiesysteem wordt verstaan: het samenhangend geheel van gegevensverzamelingen en de daarbij behorende personen, procedures, processen en programmatuur, alsmede de voor het informatiesysteem getroffen voorzieningen voor opslag, verwerking en communicatie.

4.1.3 Beheersmaatregelen

Specifiek voor security monitoring stelt het CBS de onderstaande additionele maatregelen vast, om de gegevens op een juiste manier af te screenen. De volgende governance maatregelen zijn van toepassing op alle security monitoring-diensten van het CBS:

1. Binnen het CBS is vastgesteld dat de beveiligingsprocedures binnen de directe verantwoordelijkheid van het lijnmanagement valt.
2. Het CBS controleert periodiek op naleving van de betrouwbaarheidsmaatregelen:
 - a. Ieder kwartaal wordt er een rapportage opgesteld met daarin de meldingen rondom privacy en security.
 - b. Tweejaarlijks wordt er een externe IT-beveiligingsaudit uitgevoerd.
3. Bij het CBS wordt er gewerkt volgens de ISO27001 en de BIO 2.0 norm. Het certificaat van de ISO27001-audit is terug te vinden op de website¹⁰ van het CBS. Deze audit vindt periodiek plaats door een externe partij.

¹⁰ <https://www.cbs.nl/-/media/cbs/over-ons/organisatie/standaardcbbspia-2021-v20.pdf>

4. Het CBS voert interne audits uit. Jaarlijks wordt er gerapporteerd aan de directie van het CBS. Meer informatie hierover is terug te vinden op intranet in de werkruimte Auditing¹¹.
5. Verder worden maandelijks penetratietesten (vulnerability scan) uitgevoerd op infrastructuur van het CBS. Ook worden er periodiek diepgaandere penetratietests uitgevoerd op specifieke applicaties of infrastructuur componenten.
6. De data wordt centraal opgeslagen conform de vastgestelde (wettelijke) bewaartermijnen. Zoals vastgelegd in het beleid en conform de termijnen benoemd in onderdeel A paragraaf 1.10 van dit document.
7. Bij het introduceren van nieuwe security monitoringsdiensten dient er een onboardingprocedure worden vastgesteld voor de data die benodigd is voor deze dienst. Deze procedure dient de volgende zaken te borgen: De benodigde data dient te worden beoordeeld of dat deze noodzakelijk is en of dat deze in de vastgelegde standaard valt, zoals uiteengezet is in dit document, of dat een additionele DPIA benodigd is waarin additionele maatregelen zoals data masking of pseudonimiseren worden vastgelegd. In deze procedure dient ook geborgd te zijn dat de rechten op basis van RBAC worden ingericht. Het RBAC model dient gedocumenteerd te zijn.
8. Op basis van het onboardingsproces kan het noodzakelijk zijn om additionele veiligheidsmaatregelen te nemen voor specifieke data. De additionele maatregelen worden in aparte DPIA vastgelegd hier worden vervolgens de extra maatregelen vastgelegd zoals data masking en pseudonimiseren. De noodzaak hiervan zal per afwijkend data type moeten worden bepaald. Omdat er een DPIA gemaakt wordt voor deze uitzondering zullen hierin alle betrokken partijen (FG, CPO, Legal) moeten worden gekend.
9. Werknemers van het CBS krijgen alleen toegang tot de data relevant voor de taken die ze moeten uitvoeren. Hiervoor wordt er gebruik gemaakt van Role Based Access Control.
10. Usecases dienen ten alle tijden via het vier ogen principe te worden opgesteld en mogen alleen met goedkeuring van de lijnmanager geactiveerd te worden.

4.2 Maatregelen per risico

Naast de algemene CBS brede maatregelen beschreven in de voorgaande paragraaf worden onderstaand de maatregelen per risico uiteengezet.

Risico 1a tm b:

De stappen in het onboarding proces borgen de doelbinding, proportionaliteit en noodzaak voor het gebruik van de benodigde data. Data die niet binnen de afgesproken standaard valt dient via goedkeuring van een additionele DPIA waarbij indien nodig de CPO, FG en OR worden gekend.

Risico 2 a tot en met d:

De rechtscheiding op basis van RBAC in te richten zorgen we voor een adequate verdeling in rechten, inzicht in en verwerking van persoonsgegevens. Deze rechtenstructuur is vereist voor alle security monitoringsdiensten. Deze rechtenstructuur wordt gelijksoortig ingeregeld voor alle afdelingen die toegang krijgen tot het platform. Waarbij iedere afdeling alleen maar toegang krijgt tot de data die voor die afdeling en het specifieke doel benodigd zijn. Verder worden usecases via het vier ogen principe opgesteld en alleen met goedkeuring geactiveerd.

¹¹ <https://cbsintranet/werkruimten/Auditing/default.aspx>

Bij ingebruikname van nieuwe security monitoring-tooling in de cloud, dienen passende maatregelen genomen te worden om te borgen dat het personeel van deze leverancier geen toegang heeft tot gegevens van betrokkenen. Deze maatregelen kunnen bijvoorbeeld inhouden: leveren van een SOC2-type 2 verklaring, contractafspraken etc.

Risico 3a tot en met c:

De procedures rondom het afhandelen van incidenten zijn binnen het SOC vastgelegd. Deze procedure haakt vervolgens aan op de standaard (security) incident afhandeling van het CBS.

Risico 4a

De data dient versleuteld te worden opgeslagen. Het systeem dient voor communicatie verder alleen beveiligde protocollen (D.w.z. bijv. HTTPS i.p.v. HTTP) te gebruiken met uitzondering van gevallen waar dit technisch niet mogelijk is. Door deze maatregelen is de data niet zonder ontsluiting in te zien.

Risico 5a:

Elk security monitorings platform dient auditlogging te hebben waar periodiek (een keer per kwartaal) een rapport van wordt gemaakt die gedeeld wordt met de CPO, FG, CISO. Dit om borging te hebben dat er geen mensen misbruik maken van de aan hun toegekende rechten. Ook dient er gemonitord te worden op het oneigenlijk toekennen van rechten aan gebruikersaccounts en groepen.