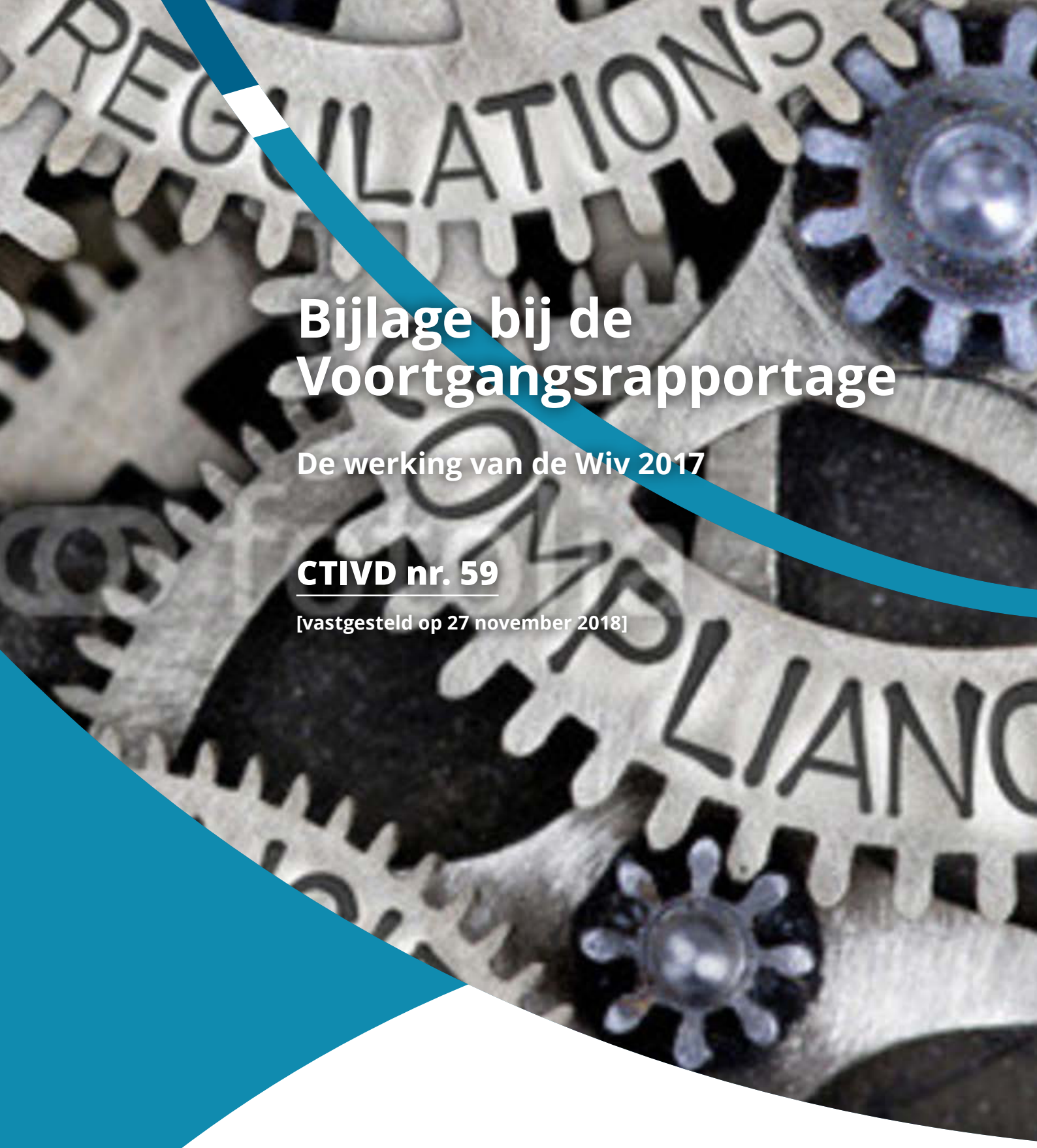

Bijlage bij de Voortgangsrapportage

De werking van de Wiv 2017

CTIVD nr. 59

[vastgesteld op 27 november 2018]

Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten

Commissie van Toezicht
op de Inlichtingen- en
Veiligheidsdiensten

CTIVD nr. 59

BIJLAGE VOORTGANGSRAPPORTAGE

De werking van de Wiv 2017

Inhoudsopgave

CTIVD nr. 59

BIJLAGE VOORTGANGSRAPPORTAGE

De werking van de Wiv 2017

1 Nulmeting Zorgplicht

Inleiding

De zorgplicht van de AIVD en de MIVD voor een rechtmatige gegevensverwerking is een essentiële waarborg voor zowel de gegevensbescherming als het toezicht daarop. De zorgplicht kent op basis van artikel 24 Wiv 2017 een viertal elementen. De beide diensten moeten door het nemen van technische, personele en organisatorische maatregelen doorlopend zorgdragen voor:

1. de bevordering van de juistheid en de volledigheid van de gegevens die worden verwerkt;

2. de bevordering van de kwaliteit van de gegevensverwerking, waaronder begrepen de daarbij gehanteerde algoritmen en modellen;

3. de beveiliging van de gegevensverwerking tegen verlies of aantasting van gegevens en tegen onbevoegde gegevensverwerking;

4. de aanwijzing van personen die bij uitsluiting van anderen bevoegd zijn bepaalde werkzaamheden te verrichten.

Het tweede element, de bevordering van de kwaliteit van de gegevensverwerking, is nieuw ten opzichte van de oude Wiv 2002. Dit onderdeel is in de Wiv 2017 opgenomen omdat meer en meer sprake is van geautomatiseerde gegevensverwerking door de diensten. Door de complexiteit die dit met zich meebrengt, is het belang van een gedegen invulling van de zorgplicht toegenomen. De toepassing van algoritmen en modellen verdient in dat kader specifieke aandacht van zowel de diensten als de toezichthouder.

De CTIVD vindt het t.a.v. de zorgplicht noodzakelijk, dat de diensten ten minste een toetsbaar overkoepelend (beleids)kader hanteren met inachtneming ook van de algemene beginselen van gegevensbescherming waaronder die van *data protection by design* en van *data protection by default*. Ook zullen de diensten in kaart moeten brengen waar rechtmatigheidsrisico's aan de orde zijn in hun interne processen van gegevensverwerking en een systematiek van interne controle toepassen (zoals accreditatie, assessments en audits). Het gaat hier om noodzakelijke voorwaarden om op een gedegen wijze invulling te kunnen geven aan hun zorgplicht en de CTIVD in staat te stellen op de naleving daarvan effectief toezicht uit te oefenen. Een keuze voor algemeen erkende instrumenten daarbij ligt voor de hand, omdat deze in de gehele private- en overheidssector eveneens worden toegepast als

gevolg van ontwikkelingen in het Europees recht op het terrein van gegevensbescherming. De keuze voor bepaalde instrumenten boven andere, en de precieze inrichting daarvan, is evenwel aan de AIVD en de MIVD. Daarbij gelden als voorwaarden dat wordt voorzien in een sluitend beleidskader en dat de instrumenten effectief toezicht op de naleving van de zorgplicht door de CTIVD mogelijk maken en daarmee ook in overleg met haar tot stand komen.

Resultaten van de nulmeting

Risico indicatie
De CTIVD karakteriseert de risico's op onrechtmatige gegevensverwerking door de AIVD en de MIVD als **hoog**.

Toelichting

De AIVD en de MIVD hebben voorafgaand aan en na de inwerkingtreding van de Wiv 2017 verbinding gezocht met de zorgplicht van artikel 24 Wiv 2017 door aan de hand van tien onderwerpen, zoals datareductie, interne autorisaties en functie- en taakscheiding, honderd maatregelen in te stellen. In oktober 2018 is aan de tien onderwerpen een elfde toegevoegd, te weten zorgplicht en *compliance*. De honderd maatregelen zien op de implementatie van de nieuwe wet en hadden hoe dan ook, ook los van de zorgplicht, genomen moeten worden. De maatregelen zien met andere woorden niet op de implementatie van de zorgplicht zelf, te weten het door middel van een algemeen aanvaard instrumentarium doorlopend interne controle uitoefenen op het op een juiste wijze uitvoering geven aan wettelijke en beleidsmatige verplichtingen binnen de organisatie (*compliance*). De AIVD en de MIVD richtten zich met hun aanpak en maatregelen weliswaar op een zekere mate van *compliance*, kern is en blijft echter dat daarmee nog niet is voorzien in een adequaat, werkend instrumentarium voor interne controle.

Geen van beide diensten had per 1 mei 2018 een kenbaar, overkoepelend (beleids)kader op het terrein van gegevensverwerking o.m. langs de lijn van *data protection by design* en *data protection by default*. Evenmin was sprake van de inrichting of toepassing van andere, breed hanteerbare instrumenten die de AIVD en de MIVD in staat stellen doorlopend interne controle uit te oefenen op de interne (technische) processen van gegevensverwerking binnen de dienst. Hier valt te denken aan de accreditatie van systemen, assessments om risico's in interne processen vast te stellen, audits om de werking van systemen te toetsen, de inrichting van een *compliance* functie etc.

De elementen van de zorgplicht die al bestonden in de oude Wiv 2002 zijn over het algemeen ingebed in de gegevensverwerkingsprocessen van de diensten. Bovendien zijn aanvullende maatregelen ingesteld na de inwerkingtreding van de Wiv 2017. Zo wordt door de beide diensten veel waarde gehecht aan bepaalde elementen van gegevensbescherming, o.m. de beveiliging van gegevens, functie- en taakscheiding en interne compartimentering (*need to know* principe). Ook zijn de interne processen van de diensten mede gericht op het bevorderen van de juistheid en volledigheid van de gegevens, o.m. door te borgen dat herleidbaar is wanneer gegevens verzameld zijn en waar gegevens vandaan komen. Dit gebeurt bijvoorbeeld door het labelen van gegevens nadat deze zijn verworven. De technologische ontwikkeling en de nieuwe bevoegdheden en verplichtingen van de diensten onder de Wiv 2017 brengen t.a.v. de al bestaande elementen van de zorgplicht wel nieuwe uitdagingen met zich mee (zie ook paragraaf 2 over datareductie).

De zorgplicht zoals neergelegd in de Wiv 2017 vraagt om een breed toepasbaar instrumentarium waarmee de AIVD en de MIVD in staat zijn controle uit te oefenen over al hun processen van gegevensverwerking in brede zin.

De AIVD heeft inmiddels onderkend dat een verdere uitwerking van de zorgplicht in beleid en werkinstructies noodzakelijk is. Een beleidskader voor gegevensbescherming is sinds oktober 2018 beschikbaar m.b.t. een systematiek van interne controle, langs de lijn van risicoanalyses, assessments en audits. Verder heeft de AIVD in oktober 2018 een portefeuillehouder zorgplicht en compliance aangesteld, die het systeem voor compliance management gaat versterken, wordt een auditinstrumentarium ontwikkeld en zijn een tweetal privacy experts aangesteld.

De MIVD heeft in oktober 2018 aangegeven beleid te zullen maken waarin herkenbaar verbinding wordt gelegd met de beginselen van *dataprotection by design* en *dataprotection by default*. Dit beleidskader is thans gereed. Een systematiek voor interne controle is niet in beleid vervat. Op operationeel/tactisch niveau wordt binnen de MIVD gewerkt aan de uitwerking van compliance en audits, maar dit verkeert nog in een conceptuele fase. Een daadwerkelijke inrichting van een instrumentarium is niet op de korte termijn voorzien en hangt samen met een benodigde versterking van de ICT infrastructuur van de MIVD.

Door de beide ministers is aan de CTIVD aangegeven dat momenteel wordt gewerkt aan de ontwikkeling van instrumenten voor de zorgplicht. Deze instrumenten moeten de diensten (centraal) zicht geven op de werking van processen en systemen van gegevensverwerking en hen daardoor in staat stellen risico's te signaleren en tijdig maatregelen te nemen. De beide ministers stelden dat het kunnen voldoen aan de wettelijke taken en de operationele taakuitoefening bij de inrichting van het instrumentarium voor de zorgplicht leidend zal zijn. Naar het oordeel van de CTIVD dienen adequate interne controle en randvoorwaarden voor effectief extern toezicht daarbij leidend te zijn. In dat verband is het van essentieel belang dat het instrumentarium voor de zorgplicht op een zo kort mogelijk termijn concreet wordt ingericht en geïmplementeerd. Dit vraagt om een tijdsplanning waaruit het belang van de zorgplicht blijkt. Die tijdsplanning is nu niet voorzien bij de beide diensten.

2 Nulmeting Datareductie

Inleiding

De verplichting tot permanente datareductie vormt de hoeksteen van de privacybescherming in de Wiv 2017. Kortgezegd komt het erop neer dat de AIVD en de MIVD de gegevens die zij verzamelen d.m.v. bijzondere bevoegdheden zo spoedig mogelijk op relevantie moeten beoordelen. Niet relevante gegevens moeten terstond en onomkeerbaar worden vernietigd. Gegevens die niet zijn beoordeeld op relevantie moeten binnen een jaar na verwerving zijn vernietigd. Dit is neergelegd in artikel 27 Wiv 2017.

Voor gegevens verzameld via onderzoeksopdrachtgerichte interceptie geldt een afzonderlijke regeling die wordt besproken in paragraaf 5. Hier gaat het dus uitsluitend om datareductie van gegevens verzameld via bijzondere bevoegdheden zoals gericht tappen, hacken, het opvragen van opgeslagen gegevens etc. Ook bij deze bevoegdheden kan het gaan om de verzameling van zeer grote hoeveelheden gegevens, waarvan een deel ziet op personen en organisaties waarnaar de diensten geen onderzoek verrichten. Een rechtmatige datareductie is in dat kader essentieel.

De verplichting tot datareductie kent enkele cruciale onderdelen die nadere invulling dienen te krijgen in beleid en werkprocessen van de beide diensten:

1. Wat wordt verstaan onder relevante gegevens en wat niet?

2. Welke beoordelingstermijn wordt gehanteerd?

3. Op welke wijze vindt datareductie plaats?

4. Hoe wordt gegarandeerd dat gegevens onomkeerbaar worden vernietigd wanneer dat door de wet wordt vereist?

Resultaten van de nulmeting

1. Wat wordt verstaan onder relevante gegevens en wat niet?

Risico indicatie
De CTIVD beoordeelt het risico in deze voor beide diensten als **beperkt**.

Toelichting

In het beleid van de AIVD en de MIVD is opgenomen dat gegevens relevant zijn wanneer zij betekenis hebben voor het onderzoek. Gegevens kunnen in positieve of negatieve zin bijdragen aan de beantwoording van onderzoeksvragen. Gegevens kunnen ook als relevant beoordeeld worden wanneer de gegevens sturing, richting en duiding geven aan het onderzoek. De CTIVD vindt het begrijpelijk dat een breed relevantiebegrip wordt gehanteerd, gelet op het belang daarvan voor het inlichtingenproces. Van belang is ook dat sprake is van een objectieve relevantiebeoordeling. De beide diensten onderschrijven dit inmiddels. Een objectieve beoordeling wil zeggen dat een persoon buiten het operationele proces, in het kader van interne controle of extern toezicht, moet kunnen begrijpen waarom gegevens relevant zijn beoordeeld. Is dat niet aanstonds duidelijk, dan vereist dit een aanvullende motivering van de diensten. Daarbij kan bijvoorbeeld worden gedacht aan gegevens die alleen van belang zijn voor de uitvoering van een operationele actie. Zo kan het bij de inzet van een bijzondere bevoegdheid soms cruciaal zijn om te weten wanneer de buren van een target thuis zijn, maar heeft dit geen betekenis voor het onderzoek naar het target als zodanig. Ook informatie die personen of organisaties als target uitsluiten, kan onder dit type relevante gegevens worden

geschaard. De diensten dienen in hun beleid en werkinstructies vast te leggen dat sprake dient te zijn van een objectieve relevantiebeoordeling, nader te omschrijven in welke gevallen een aanvullende motivering van belang is en hoe dit dient te worden vastgelegd. Dit is vooralsnog niet gebeurd.

2. Welke beoordelingstermijn wordt gehanteerd?

Risico indicatie
Het risico wordt voor beide diensten ingeschat als **gemiddeld**.

Toelichting

Het begrip 'zo spoedig mogelijk' is niet uitgewerkt in het interne beleid of in werkinstructies van de AIVD of de MIVD. De diensten achtten dit niet nodig, omdat de beperkte duur van de inzet van bijzondere bevoegdheden (doorgaans drie maanden) en de verplichting om bij de verlening daarvan over de opbrengst te rapporteren, een spoedige beoordeling van de gegevens vereist. Het zo spoedig mogelijk beoordelen van de relevantie ligt met andere woorden besloten in het inlichtingenproces. De CTIVD onderschrijft dat dit het geval is, maar signaleert dat ook sprake is van situaties waarbij geen verlenging aan de orde is. Een veel voorkomend voorbeeld is de eenmalige inzet van een hack, waarbij in voorkomende gevallen een grote hoeveelheid gegevens kan worden overgenomen door de diensten. Ook voor dergelijke situaties dienen het beleid en de werkinstructies van de diensten de medewerker handvatten te geven wat een zo spoedig mogelijke beoordeling van relevantie inhoudt. Een enkel opnemen van de verplichting dat gegevens zo spoedig mogelijk op relevantie beoordeeld moeten worden, zonder dat dit nader wordt geëxpliciteerd, biedt daarin geen houvast.

Een belangrijk aandachtspunt is ook dat 'oude data', gegevens die zijn verzameld op basis van de Wiv 2002, eveneens zo spoedig mogelijk op relevantie dienen te worden beoordeeld. De beide diensten hebben hier nog geen regeling voor vastgelegd, anders dan dat niet beoordeelde 'oude data' op 1 mei 2019 vernietigd moeten worden. Ook hier dient het wettelijke vereiste van een 'zo spoedig mogelijke' beoordeling van de relevantie van gegevens zijn werking te hebben. Eind oktober 2018 is door de AIVD en de MIVD een aanvang gemaakt met het op relevantie beoordelen van 'oude data'.

3. Op welke wijze vindt datareductie plaats?

Risico indicatie
Het risico wordt voor de AIVD nu ingeschat als **gemiddeld**. Voor de MIVD beoordeelt de CTIVD het risico als **hoog**.

Toelichting

De relevantiebeoordeling vindt bij de AIVD met geautomatiseerde ondersteuning (impliciet) of handmatig (expliciet) plaats. De AIVD heeft een systematiek van relevantiebeoordeling ontwikkeld die in belangrijke mate in technische zin wordt ondersteund. Dit is geen eenvoudige opgave geweest. In het beleid van de AIVD is echter beperkt ingekaderd in welke gevallen en met toepassing van welke voorwaarden de relevantiebeoordeling met geautomatiseerde ondersteuning kan plaatsvinden. De gerichtheid van de inzet van een bevoegdheid vormt een graadmeter daarbij, maar een verdere afbakening is niet aan de orde. Evenmin wordt bij de keuze voor een beoordeling met geautomatiseerde ondersteuning een interne onderbouwing daarvoor gevraagd. De AIVD heeft vooralsnog onvoldoende helder vastgelegd in welke gevallen relevantiebeoordeling met geautomatiseerde ondersteuning geoorloofd is en hoe deze methode van relevantiebeoordeling zich verhoudt tot handmatige relevantiebeoordeling. Relevantiebeoordeling met behulp van een geautomatiseerd systeem houdt bijvoorbeeld in dat bepaalde gegevens met een bepaald kenmerk automatisch als relevant worden beoordeeld. Dit is veelal niet hetzelfde als handmatige relevantiebeoordeling, waar sprake is van een

inhoudelijke beoordeling van de gegevens, en kan bovendien andere risico's met zich meebrengen. In veel gevallen zal relevantiebeoordeling met een geautomatiseerd systeem slechts leiden tot de potentiële of waarschijnlijke vaststelling van de relevantie in plaats van de daadwerkelijke vaststelling daarvan. Dit vereist nadere inkadering in het beleid van de AIVD, omdat hiermee niet zonder meer wordt voldaan aan de wettelijk vereiste relevantiebeoordeling.

Verder is van belang dat de relevantiebeoordeling herleidbaar is, zowel voor interne controle als extern toezicht. Dit betekent dat het kenbaar moet zijn waar gegevens vandaan komen, wanneer de relevantie is vastgesteld en waar de relevantie op is gebaseerd. De basis voor relevantie kan bijvoorbeeld een concreet uitgewerkte onderzoeksvraag zijn, een verzoek om toestemming voor de inzet van een bevoegdheid of een aanvullende motivering. Interne controle op de relevantiebeoordeling, bijvoorbeeld in de vorm van audits, ontbreekt vooralsnog. De AIVD heeft wel plannen voor het inrichten van interne controle op relevantiebeoordeling d.m.v. audits. Deze plannen bevinden zich echter nog in een conceptuele fase. Effectief toezicht op het beoordelen van relevantie is daarmee vooralsnog niet mogelijk.

De MIVD heeft een eenvoudiger systematiek van relevantiebeoordeling, die in beperktere mate technisch wordt ondersteund. Werkinstructies voor het beoordelen van relevantie per bijzondere bevoegdheid zijn in oktober 2018 beschikbaar gesteld aan medewerkers. Het ontbreekt de MIVD echter aan een passende ICT infrastructuur als basis voor een meer gestructureerde datareductie systematiek. Voor een aantal systemen van gegevensverwerking is *data lineage* (oorsprong en verloop van data) niet op orde. Er dient een oplossing gevonden te worden om systemen sluitend te maken en te voorkomen dat gegevens tussen wal en schip raken. Momenteel is de MIVD bezig met het ontwikkelen van (tijdelijke) beleidsmatige oplossingen voor deze systemen. Een interne controle systematiek is niet voorzien en, gelet op de ICT infrastructuur, nu niet realiseerbaar. Effectief toezicht op de relevantiebeoordeling is daarmee niet mogelijk.

De minister van Defensie heeft aan de CTIVD aangegeven dat het realiseren van een ICT-infrastructuur voor datareductie bij de MIVD, een traject is dat meerdere jaren zal vergen. Een adequate technische oplossing voor datareductie zou een ideale situatie betreffen. Het ontbreken hiervan betekent volgens de minister niet dat extern toezicht niet aan de orde kan zijn. De CTIVD benadrukt dat, gegeven de enorme omvang van de te verwerven data (bulk), een gedegen systematiek van datareductie is vereist om invulling te kunnen geven aan de wettelijke verplichting van datareductie. Dit dient niet alleen zijn weerslag te krijgen in beleid en werkinstructies, maar dient ook in technische zin goed te zijn ingebed in de systemen. Een adequate technische oplossing voor datareductie is met andere woorden een basisvoorwaarde voor het kunnen bereiken van een rechtmatige situatie bij de MIVD. Dat de invoering zich over meerdere jaren kan uitspreiden levert het risico op van een even zo lange onrechtmatige handelwijze van de MIVD, hetgeen niet acceptabel is. Het is bovendien een basisvoorwaarde voor de doorlopende interne controle die de MIVD dient te hebben op de werking van de systematiek van datareductie. Zonder de aanwezigheid van interne controle mechanismen, is ook effectief extern toezicht niet aan de orde.

4. Hoe wordt gegarandeerd dat gegevens onomkeerbaar worden vernietigd wanneer dat door de wet wordt vereist?

Risico indicatie
Het risico wordt voor de AIVD nu ingeschat als **gemiddeld**. Voor de MIVD beoordeelt de CTIVD het risico als **hoog**.

Toelichting

Vernietiging hangt samen met relevantiebepaling en met het verstrijken van de bewaartermijn. Niet relevante gegevens moeten terstond worden vernietigd en niet beoordeelde gegevens moeten zijn vernietigd wanneer de termijn van een jaar (met een eventuele verlenging van zes maanden) verloopt. Voor de tijdige vernietiging van gegevens is het, gegeven de omvang daarvan, absoluut noodzakelijk dat sprake is van een ICT infrastructuur die hier in kan voorzien.

Bij de AIVD lijkt dat het geval. Gegevens worden bij binnenkomst gelabeld en voorzien van een datumstempel. De relevantiebepaling wordt in die zin technisch ondersteund dat gegevens die als niet relevant zijn beoordeeld, terstond zouden moeten worden vernietigd. Ditzelfde geldt voor gegevens waarvan de bewaartermijn is verlopen. Tot op heden is de mogelijkheid gegevens niet-relevant te verklaren echter in veel gebruikte applicaties nog niet aanwezig. Een mechanisme voor interne controle ontbreekt. Plannen voor het verrichten van audits t.a.v. de vernietiging van gegevens zijn nog onvoldoende concreet. De vernietiging van gegevens is zonder interne controle door de AIVD niet goed toetsbaar door de CTIVD.

De ICT infrastructuur van de MIVD maakt dat een rechtmatige vernietiging van gegevens onvoldoende gewaarborgd is. Dit dient te worden opgevangen door een toereikend systeem van interne controle. Dit is thans niet het geval en is ook niet eenvoudig gelet op de beperkte ICT mogelijkheden van de MIVD. Het is hierdoor niet mogelijk effectief extern toezicht te houden op de vernietiging van gegevens door de MIVD.

3 Nulmeting Onderzoeksopdrachtgerichte interceptie

Inleiding

In de artikelen 48 t/m 50 van de Wiv 2017 is de bevoegdheid van onderzoeksopdrachtgerichte interceptie (OOG interceptie) opgenomen. Met deze bepalingen is het wettelijk kader voor bulkinterceptie van de ether aangescherpt en is de mogelijkheid gecreëerd ook bulkinterceptie op de kabel toe te passen. Deze nieuwe bevoegdheid heeft een aanzienlijke politieke en maatschappelijke discussie in Nederland te weeg gebracht, gedurende het wetgevingsproces en daarna in de aanloop naar het raadgevend referendum dat over de Wiv 2017 is gehouden in maart van dit jaar. Deze discussie centreerde zich rond het beeld dat sprake zou zijn van een 'sleepnet'.

De AIVD en de MIVD zijn momenteel volop bezig met het operationaliseren van de onderzoeksopdrachtgerichte interceptie op de kabel. Het was tot dusver nog te vroeg om t.a.v. deze bevoegdheid een nulmeting te verrichten. De CTIVD richt zich daarom eerst op de inzet van de onderzoeksopdrachtgerichte interceptie van de ether.

De CTIVD heeft in de nulmeting specifiek aandacht gehad voor de wijze waarop de wettelijke waarborgen invulling hebben gekregen bij OOG interceptie van de ether (en straks ook toegepast moeten worden bij OOG interceptie op de kabel). De volgende vragen zijn van belang:

1. Is het toestemmingsproces adequaat ingericht?
2. Wordt toepassing gegeven aan het criterium 'zo gericht mogelijk'?
3. Zijn voldoende waarborgen voor geautomatiseerde data-analyse aan de orde?
4. Is sprake van voldoende waarborgen voor de selectie van gegevens?
5. Wordt invulling gegeven aan een verantwoorde databeperking?
6. Is functie- en taakscheiding gewaarborgd waar dit vereist is?

Resultaten van de nulmeting

1. Is het toestemmingsproces adequaat ingericht?

Risico indicatie
De CTIVD ziet hier **geen** risico op onrechtmatig handelen door de diensten.

Toelichting

De diensten hebben algemeen beleid op het terrein van OOG interceptie, de verschillende fasen die in dat kader aan de orde zijn en de bevoegdheden die daarbij kunnen worden ingezet. Het beleid biedt houvast voor het opstellen van verzoeken om toestemming.[1] Er is sprake van formats voor verzoeken om toestemming, waarin alle wettelijke vereisten die moeten worden ingevuld of gemotiveerd, zijn opgenomen. De formats bevatten bepaalde standaard passages en voorbeelden van motiveringen.

1 Op andere onderdelen biedt het algemeen beleid onvoldoende houvast. Dit wordt hieronder per onderwerp besproken.

De CTIVD heeft een steekproef uitgevoerd naar de verzoeken om toestemming die zijn getoetst door de TIB en al dan niet rechtmatig zijn bevonden. Veel verzoeken zijn combinatieverzoeken van ofwel interceptie en search gericht op interceptie, ofwel selectie en search gericht op selectie. Dit is conform de gegeven toelichting op de Wiv 2017 en het interne beleid van de diensten. Voor de inzet van geautomatiseerde data-analyse zijn afzonderlijke verzoeken ingediend. De verzoeken die door de TIB rechtmatig zijn bevonden, bevatten alle wettelijk vereiste elementen. De CTIVD heeft in deze nulmeting geen aanleiding gezien te toetsen of de verzoeken op inhoud voldoen aan de vereisten van de wet. Die beoordeling is in beginsel aan de TIB.

2. Wordt toepassing gegeven aan het criterium 'zo gericht mogelijk'?

Risico indicatie
De CTIVD constateert dat sprake is van een **hoog** risico.

Toelichting

In het beleid of de werkinstructies van de AIVD en de MIVD wordt niet ingegaan op het criterium 'zo gericht mogelijk'. Het is de CTIVD onduidelijk gebleven hoe dit in de praktijk tot uiting komt. Het criterium 'zo gericht mogelijk' wordt door de beide diensten wel gehanteerd in aanvragen tot toestemming voor de onderzoeksopdrachtgerichte interceptie van gegevens die via de ether verlopen, maar het beleid, de werkinstructies en de feitelijke werkprocessen van de beide diensten maken niet duidelijk hoe 'zo gericht mogelijk' in de praktijk uitwerking krijgt. Het criterium heeft, met andere woorden, geen herkenbare invulling gekregen door de AIVD en de MIVD.

Binnen het stelsel van onderzoeksopdrachtgerichte interceptie is sprake van verschillende stadia waarin de diensten zich richten op de interceptie en verdere verwerking van aan de onderzoeksopdrachten gerelateerde data. Zo worden gegevens bij interceptie gefilterd om te bepalen welke gegevens worden opgeslagen en welke worden vernietigd. Verder is sprake van de toekenning van selectiecriteria voor het selecteren van inhoud van communicatie die beschikbaar wordt gesteld aan de operationele teams. Ook wordt geïntercepteerde metadata geautomatiseerd geanalyseerd. Elk van deze onderdelen van het interceptieproces dient 'zo gericht mogelijk' plaats te vinden. Aan de hand hiervan wordt immers bepaald welke gegevens worden opgeslagen voor nadere verwerking en van welke gegevens (inhoudelijk) kennis mag worden genomen ten behoeve van gebruik in het operationeel proces. Concreet houdt dit in dat o.m. de filtering van te intercepteren gegevens, de toekenning van selectiecriteria en bijvoorbeeld het gebruik van een profiel bij metadata-analyse 'zo gericht mogelijk' moeten zijn.

3. Zijn voldoende waarborgen voor geautomatiseerde data-analyse aan de orde?

Risico indicatie
De CTIVD beordeelt het risico op onrechtmatig handelen voor beide diensten als **hoog**.

Toelichting

De AIVD en de MIVD moeten toestemming vragen voor de geautomatiseerde analyse van gegevens die zijn verkregen door OOG interceptie (metadata-analyse), wanneer de analyse is gericht op het identificeren van personen of organisaties. Hier doen zich twee vragen voor: 1) Wanneer is sprake van geautomatiseerde analyse? 2) Wanneer is dit gericht op het identificeren van personen of organisaties. Met andere woorden, in welke gevallen moet toestemming worden verkregen en in welke gevallen niet?

De CTIVD heeft vastgesteld dat de beide diensten per 1 mei 2018 geen beleid hadden dat een toereikend antwoord gaf op deze vragen. Evenmin kon op basis van de inrichting van werkprocessen van de diensten vastgesteld worden voor welke gevallen wel of geen toestemming diende te worden verkregen. De CTIVD stelde m.b.t. de periode 1 mei tot 1 juli 2018 vast dat het proces van geautomatiseerde data-analyse met onvoldoende waarborgen was omkleed, o.m. door het ontbreken van een heldere definiëring van metadata en van gerichtheid op identificeren, onduidelijkheden rond de kwaliteit van analysetools en een ruime toegang tot metadata vanuit het operationeel teamproces. Evenmin is sprake van mechanismen van interne controle door de diensten op dit proces, wat, samen met een gebrekkige schriftelijke of anderszins zichtbare invulling van wettelijke verplichtingen, een hoog risico op onrechtmatig handelen door de beide diensten oplevert.

De CTIVD heeft daarop besloten het onderwerp verder uit te diepen in rechtseenheid overleg met de TIB, ten einde te komen tot de gezamenlijke vaststelling van de interpretatie die zij geven aan de wet. In dat verband heeft nader overleg plaatsgevonden met de departementen van BZK en van Defensie en met de AIVD en de MIVD. Dit heeft geleid tot nadere toezeggingen m.b.t. de motivering van de inzet, de inrichting en de toepassing van geautomatiseerde data-analyse. De CTIVD ziet dit als een positieve ontwikkeling. Een fundamenteel verschil bleef echter een door de diensten aangebracht en door de ministers onderschreven onderscheid tussen eenvoudige en complexe metadata-analyses, waarbij alleen de meer complexe metadata-analyses onder het bereik van voorafgaande toestemming van de minister en toetsing door de TIB zouden vallen.

De TIB en CTIVD zijn van oordeel dat, gelet op de huidige wettelijke regeling en de toelichting daarop,[2] elke metadata-analyse onder het bereik van de desbetreffende bepaling valt. Voorafgaande toestemming van de minister en toetsing daarvan door TIB wordt alleen vereist wanneer de geautomatiseerde metadata-analyse is gericht op het identificeren van personen en organisaties. Dit laat de diensten ruimte voor het zonder voorafgaande toestemming verrichten van metadata-analyse ten aanzien van reeds geïdentificeerde personen en organisaties. Het aanvullend aanbrengen van een onderscheid tussen eenvoudige en complexe vormen van metadata-analyse zou leiden tot een ongeoorloofde inperking van de privacybescherming.

De TIB en de CTIVD hebben op 26 oktober 2018 hun concluderende standpunt in een rechtseenheid brief kenbaar gemaakt aan de ministers van BZK en Defensie en aan de beide diensthoofden. Ook hebben zij naar aanleiding van de recente uitspraak van het Europees Hof voor de Rechten van de Mens (EHRM) in de zaak Big Brother Watch aanbevolen de wet aan te passen waar het gaat om de wettelijk vastgelegde gerichtheid op het identificeren van personen en organisaties. Op 23 november is een overeenkomstige versie van deze rechtseenheid brief verzonden aan de Eerste en Tweede Kamer en gepubliceerd op de websites van de TIB en de CTIVD. De rechtseenheidbrieven van de TIB en de CTIVD zijn, vanuit het uitgangspunt van een redelijke wetsinterpretatie, voor de diensten kader scheppend m.b.t. de uitvoering van de wet.

De CTIVD heeft in oktober en november 2018 een technische steekproef uitgevoerd naar de feitelijke toepassing van geautomatiseerde metadata-analyse in het kader van onderzoeksopdrachtgerichte interceptie door de beide diensten vanaf 1 mei 2018. Met de steekproef beoogde de CTIVD twee vragen te beantwoorden: 1) Welke vormen van geautomatiseerde metadata-analyse zijn door de AIVD en de MIVD toegepast vanaf 1 mei 2018? 2) Is de CTIVD in staat hierop effectief toezicht uit te oefenen? De aard van dit technisch onderzoek is wezenlijk anders dan het reguliere diepteonderzoek dat de CTIVD uitvoert. De steekproef is gericht op de technische werking van gegevensverwerkingssystemen en een reconstructie van data analyse handelingen aan de hand van onder meer loggegevens van de AIVD en de MIVD zelf. De resultaten van deze steekproef zijn inmiddels bekend. De CTIVD stelt de

2 Zo wordt in de parlementaire behandeling van de Wiv 2017 duidelijk gemaakt dat elke vorm van metadata-analyse geautomatiseerde data-analyse is; *Kamerstukken II* 2017/18, 34588, nr. 3, p. 112.

beide diensten en departementen eerst in de gelegenheid op de bevindingen te reageren, voordat zij deze publiekelijk kenbaar maakt.

4. Is sprake van voldoende waarborgen voor de selectie van gegevens?

Risico indicatie
De CTIVD beoordeelt het risico voor beide diensten als **beperkt**.

Toelichting

De beide diensten hebben uitgebreid beleid opgesteld over de inzet van selectie. De wettelijke vereisten zijn daarin vastgelegd en worden nader toegelicht. Door het selecteren van gegevens aan de hand van selectiecriteria wordt de inhoud van deze gegevens toegankelijk gemaakt voor medewerkers in het operationele proces. Het bepalen van de selectiecriteria, zoals telefoonnummers, IP-adressen en trefwoorden, gebeurt intern. Daarvoor hoeft geen voorafgaande externe toestemming te worden verkregen. De selectiecriteria dienen wel intern gemotiveerd en geautoriseerd te worden. Uit mandaatregelingen blijkt welke functionaris bevoegd is tot het vaststellen van selectiecriteria. Voor het intern aanvragen van selectiecriteria bestaan echter nog geen werkinstructies waarin is opgenomen hoe dit dient plaats te vinden.

Bij de beide diensten was evenmin sprake van een werkinstructie voor het verwijderen van selectiecriteria, bijvoorbeeld in het geval met een bepaald selectiecriterium onvoldoende relevante gegevens worden geselecteerd. De MIVD heeft in oktober 2018 een werkinstructie voor het verwijderen van selectiecriteria voor het verwerkingssysteem aan de CTIVD ter beschikking gesteld. De CTIVD is positief over de werkinstructie. Wel mist nog een verwijzing naar en toelichting op deze werkinstructie in het algemeen beleid.

5. Wordt invulling gegeven aan een verantwoorde databeperking?

Risico indicatie
De CTIVD beoordeelt het risico hier als **hoog**.

Toelichting

Databeperking vindt in het interceptieproces getrapt plaats. Filtering bepaalt welke gegevens worden opgeslagen en welke niet. Na filtering geldt een doorlopende vernietigingsplicht t.a.v. de opgeslagen gegevens. Dat wil zeggen dat wanneer gegevens nader worden verkend o.b.v. artikel 49 Wiv 2017 of metadata geautomatiseerd worden geanalyseerd o.b.v. artikel 50 lid 1 onder b Wiv 2017, de diensten die gegevens moeten vernietigen waarvan zij constateren dat deze niet relevant zijn voor enig lopend onderzoek. Een volgende stap in databeperking is het op relevantie beoordelen van gegevens nadat deze zijn geselecteerd op basis van selectiecriteria, zoals telefoonnummers, IP adressen of trefwoorden. De geselecteerde gegevens moeten worden beoordeeld op relevantie voor enig lopend onderzoek. Geselecteerde gegevens die niet relevant zijn, moeten worden vernietigd. De laatste stap betreft de vernietiging van niet op relevantie beoordeelde geïntercepteerde gegevens bij het aflopen van de bewaartermijn. Voor OOG interceptie van de ether geldt een bewaartermijn van maximaal drie jaar.

De CTIVD heeft vastgesteld dat er bij de AIVD en de MIVD geen specifiek beleid en werkinstructies zijn vastgesteld voor databeperking binnen het interceptiestelsel. Bij de MIVD is in beleid en werkinstructies zeer beperkt (nog onvoldoende) uitvoering gegeven aan de doorlopende vernietigingsplicht. Het is daarmee onvoldoende helder in welke gevallen moet worden overgegaan tot vernietiging van gegevens en hoe dit plaatsvindt. De beide ministers hebben aan de CTIVD aangegeven dat de ontwikkeling

en invoering van de systematiek van datareductie in het kader van onderzoeksopdrachtgerichte interceptie zowel tijd als een fasegewijze aanpak vergen. De CTIVD begrijpt dat de inrichting van een systematiek van datareductie in het kader van onderzoeksopdrachtgerichte interceptie complex is. De Wiv 2017 is echter reeds een half jaar van kracht en verantwoorde databeperking dient dus plaats te vinden. Het is daarvoor van belang dat dit zo spoedig mogelijk zijn beslag krijgt in beleid, werkprocessen, systemen en interne controlemechanismen van de AIVD en de MIVD.

M.b.t. de plicht reeds geselecteerde gegevens op relevantie te beoordelen is het beeld van de CTIVD diffuus. De CTIVD heeft in verschillende intern vastgelegde documenten van de diensten aangetroffen dat gegevens die zijn geselecteerd *by default* (standaard) als relevant worden gelabeld. Mondeling is echter door de diensten bij herhaling aangegeven dat gegevens ook nadat deze zijn geselecteerd op relevantie moeten worden beoordeeld. De beide ministers hebben aan de CTIVD echter aangegeven dat relevantiebeoordeling ook plaats kan vinden *door middel van* de inzet van de selectiebevoegdheid. De CTIVD acht de waarborg van relevantiebeoordeling essentieel. Zeker wanneer selectie plaats vindt aan de hand van trefwoorden of representaties van selectiecriteria (bijvoorbeeld een telefoonnummer zonder landcode), is de opbrengst daarvan hoe dan ook ruimer dan wat relevant is voor het onderzoek. Een relevantiebeoordeling van geselecteerde gegevens is absoluut noodzakelijk.

De vernietiging van gegevens bij het aflopen van de bewaartermijn is geborgd binnen de diensten. Gegevens worden na interceptie voorzien van een datumlabel van binnenkomst. In de vernietiging van gegevens binnen drie jaar is technisch voorzien. Wel ontbreekt een systematiek van interne controle hierop. Het is noodzakelijk dat de diensten zelf controleren, bijvoorbeeld door middel van audits, dat het systeem van vernietiging werkt zoals het behoort te werken. Pas als dat aan de orde is, kan de CTIVD effectief toezicht uitoefenen op de verplichting gegevens te vernietigen. Over het nut en de noodzaak van de bewaartermijn van drie jaar kan de CTIVD zich, gegeven het beperkte tijdverloop tot nu toe, nog niet uitspreken. Dit vereist nader onderzoek op termijn.

6. Is functie- en taakscheiding gewaarborgd waar dit vereist is?

Risico indicatie
Er is sprake van een **gemiddeld** risico op onrechtmatig handelen voor beide diensten.

Toelichting

Functie- en taakscheiding wil zeggen dat slechts aan bepaalde medewerkers de bevoegdheid wordt toegekend inhoudelijk kennis te mogen nemen van bepaalde gegevens en specifieke taken worden toegewezen die niet voor anderen gelden. Deze functie- en taakscheiding is nader beschreven in beleid van de beide diensten en zorgt voor een specifiek en kenbaar onderscheid tussen medewerkers. De CTIVD heeft een beperkte steekproef verricht van de praktijk. In de praktijk is het beeld diffuser. De toegang tot gegevens (autorisatie) kan in de praktijk verschillen tussen medewerkers met een zelfde functie en taak, terwijl dit niet het geval zou moeten zijn. Bovendien dient functie- en taakscheiding ook een fysieke component te hebben, wat wil zeggen dat het niet altijd aangewezen is medewerkers met een bredere toegang tot gegevens op de werkvloer tussen medewerkers met een beperktere toegang te plaatsen. Het belang van een dergelijke fysieke scheiding vloeit logischerwijs voort uit de wettelijk vereiste functie- en taakscheiding. Een fysieke scheiding is echter niet in alle gevallen aan de orde.

Er wordt binnen de AIVD en MIVD onderscheid gemaakt tussen inhoud van communicatie en metadata. Voor het kennisnemen van de inhoud is functie- en taakscheiding ingesteld, conform de wettelijke verplichting hiertoe in de artikelen 48 en 49 Wiv 2017. Een soortgelijke wettelijke verplichting ontbreekt voor de toegang tot metadata. Voor de toegang tot metadata is slechts in beperkte mate functie- en taakscheiding ingericht. Metadata wordt niet onbeperkt, maar wel breed toegankelijk gesteld voor

medewerkers werkzaam in het operationeel proces. De analyse van metadata kan echter een ernstige inmenging op het recht op privacy van de betrokkenen met zich meebrengen. Functie-taakscheiding kan daarbij een (bovenwettelijke) waarborg vormen ter versterking van een rechtmatige toepassing van metadata-analyse. Dit is hierboven besproken onder waarborgen voor geautomatiseerde data-analyse. Het is verder van belang dat wordt vastgelegd wie wanneer toegang heeft tot welke gegevens (autorisatie) en wie er op welke wijze gebruik maakt van die toegang (logging). Pas dan is interne controle en daarmee effectief extern toezicht mogelijk.

4 Nulmeting Klachten en meldingen van misstanden

Inleiding

In het kader van deze nulmeting heeft de CTIVD zich gericht op de inrichting en de procedures bij de AIVD en de MIVD zoals deze in beleid en werkprocessen zijn vastgelegd. De werking van de procedures in de praktijk is hier buiten beschouwing gelaten. Reden hiervan is dat de CTIVD niet vooruit wil lopen op een oordeel inzake klachten die in een later stadium aan haar afdeling Klachtbehandeling worden voorgelegd.

Naar aanleiding van de resultaten van de nulmeting zijn geen verdere activiteiten nodig van de afdeling Toezicht van de CTIVD. De afdeling Klachtbehandeling zal bij de behandeling van klachten de interne procedures bij de desbetreffende dienst (ambtshalve) toetsen. Daarnaast vindt een periodiek overleg plaats met medewerkers van de diensten, die belast zijn met de behandeling van klachten en meldingen van misstanden. Op deze wijze volgt zij de ontwikkelingen in de interne procedures van de diensten.

Resultaten van de nulmeting

Risico indicatie
De CTIVD constateert dat voor beide diensten **geen** sprake is van risico's.

Toelichting

De interne beleidsregelingen voor de behandeling van klachten en van meldingen van misstanden waren op 1 mei 2018 nog niet gereed. Inmiddels is dat wel het geval. De MIVD heeft op 18 en 25 mei 2018 regelingen gepubliceerd c.q. vastgesteld. Bij de AIVD vond dit plaats op 13 en 21 juni en op 10 juli 2018. Ondanks deze vertraging heeft de CTIVD geen risico's gezien. Zij heeft geen aanwijzingen dat klagers of melders 'tussen wal en schip' zijn geraakt in de tussenliggende periode.

De regelingen zijn helder, actueel, volledig en in lijn met het wettelijk kader dat daarop van toepassing is. Bij de regelingen van de MIVD heeft de CTIVD desondanks enkele kanttekeningen geplaatst, die hebben geleid tot wijziging van de regelingen. Zowel bij de AIVD als bij de MIVD is voldoende aansluiting gevonden bij de vuistregels voor een professionele klachtbehandeling zoals vastgesteld door de Nationale ombudsman. Het gaat om de volgende vuistregels: i) wees alert op klachten en bied toegang; ii) verken het probleem van de burger; iii) los het probleem op; iv) geen oplossing, geef zo nodig een oordeel; en v) geef gemotiveerd duidelijkheid bij de afronding. Deze vijfde vuistregel vergt in het licht van de praktijk van de AIVD en de MIVD verduidelijking. Voor de diensten geldt dat zij het oordeel *zo veel als mogelijk* van een motivering moeten voorzien. Voor zover het oordeel steunt op staatsgeheime informatie zal dit in het oordeel niet worden weergegeven. Hier ontstaat een spanningsveld tussen het belang van klager inzicht te krijgen in het oordeel en de bescherming van de nationale veiligheid.

Het vastgestelde beleid geeft de medewerkers voldoende houvast te komen tot een goede behandeling van klachten en meldingen van misstanden. Bij de AIVD heeft een interne werkinstructie voor de behandeling van meldingen van misstanden langere tijd ontbroken. Dit wordt hersteld.

De CTIVD is verder nagegaan of de websites van beide diensten voldoende informatie bevatten over de behandeling van klachten en meldingen van misstanden en of er intern voldoende bekendheid is gegeven aan het kunnen melden van een misstand. Dit is het geval. Ook wordt op de websites op een juiste manier naar de CTIVD verwezen.

Tijdelijk adres:
Frederikkazerne, gebouw 35
Van Alkemadelaan 786 | 2597 Den Haag
Postbus 90701 | 2509 LS Den Haag

T 070 315 58 20 | **F** 070 381 71 68
E info@ctivd.nl | www.ctivd.nl