NOTA VAN TOELICHTING

Algemeen deel

1. Aanleiding

De Wet coördinatie terrorismebestrijding en nationale veiligheid (Stb. 2023, nr. 454) bevat de opdracht tot het stellen van regels bij algemene maatregel van bestuur ten aanzien van een aantal onderwerpen. Het betreft:

1. Regels met betrekking tot te nemen technische, personele en organisatorische maatregelen, waaronder regels over functiescheiding, autorisatie voor het gebruik van bepaalde systemen, opslag en beveiliging (artikel 3, derde lid), en;
2. Nadere regels betreffende de inhoud en wijze van uitvoering van gegevensbeschermingsaudits ten aanzien van het gebruik van de in artikel 3, eerste lid, onderdeel a, bedoelde bronnen, voor zover dit online bronnen zijn (artikel 5, derde lid).

Dit besluit voorziet in deze regels. Op beide onderwerpen zal hierna nader worden ingegaan.

2. Inhoud besluit

2.1. Systematiek begrenzingen en waarborgen

Om de regels in onderhavig besluit in de context van de Wet coördinatie terrorismebestrijding en nationale veiligheid (hierna: de wet) te kunnen plaatsen, zal hier eerst nader worden ingegaan op de kernsystematiek van de wet en de daarin opgenomen begrenzingen en waarborgen.

De wet regelt in artikel 2 de coördinatietaak van de Minister van Justitie en Veiligheid (hierna: de Minister) op het terrein van terrorismebestrijding en de bescherming van de nationale veiligheid, ten behoeve van de samenhang en effectiviteit van het beleid en de door overheidsorganisaties te nemen maatregelen. Dit met het oog op het verhogen van de weerbaarheid tegen dreigingen en risico's, het beschermen van de nationale veiligheidsbelangen en het voorkomen van maatschappelijke ontwrichting. In verband met deze coördinatietaak kan de Minister trends en fenomenen op dit terrein signaleren, analyseren en duiden. De Nationaal Coördinator Terrorismebestrijding en Veiligheid (hierna: NCTV) voert de wet uit namens de Minister. Om die reden zal in deze toelichting gesproken worden over de taakuitvoering door de NCTV. De wet regelt in artikel 3 welke gegevens voor deze taak gebruikt kunnen worden omdat deze gegevens persoonsgegevens kunnen bevatten. Ook regelt de wet aan welke organisaties gegevens kunnen worden verstrekt, ook weer omdat daarin persoonsgegevens kunnen zijn opgenomen (artikel 7 van de wet). Daarnaast bevat de wet diverse begrenzingen en waarborgen en zal er controle plaatsvinden door de Inspectie Justitie en Veiligheid op de naleving van de wet en onderhavig besluit, naast het gebruikelijke toezicht dat de Autoriteit Persoonsgegevens verricht op de naleving van de Algemene verordening gegevensbescherming (AVG). Ter versterking van het toezicht op de naleving van de AVG is daarnaast voorzien in de benoeming van een functionaris voor gegevensbescherming specifiek voor de verwerking van persoonsgegevens onder de wet.

Ten aanzien van het signaleren, analyseren en duiden van trends en fenomenen geldt dat expliciet is vastgelegd dat dit geen bevoegdheid omvat tot het doen van onderzoek gericht op personen en organisaties (artikel 2, derde lid, van de wet). Deze bepaling brengt tot uitdrukking dat de coördinatietaak en de analysewerkzaamheden die in dit kader kunnen plaatsvinden geen bevoegdheid meebrengt om de werkzaamheden te verrichten vergelijkbaar met de werkzaamheden die de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) op basis van artikel 8, tweede lid, onderdeel a, van de Wet op de op inlichtingen- en veiligheidsdiensten 2017 (Wiv 2017) kan verrichten naar – kort gezegd - het gevaar dat uitgaat van personen en organisaties voor de nationale veiligheid. Ter bescherming van personen is deze lijn doorgetrokken naar artikel 7, derde lid, van de wet, waarin is vastgelegd dat de NCTV geen analyse kan verstrekken die er vervolgens de oorzaak van is dat een persoon in verband wordt gebracht met een trend of fenomeen. Concreet betekent dit dat bijvoorbeeld een bekende jihadistische terrorist wel benoemd kan worden in een analyse, omdat het in dat geval niet de analyse is die de persoon in verband brengt met jihadisme. Daarnaast geldt ten algemene op grond van artikel 7, tweede lid, van de wet, dat bij de verstrekking van gegevens die persoonsgegevens bevatten, altijd eerst bezien wordt of deze persoonsgegevens verwijderd kunnen worden of gepseudonimiseerd. Dit zal in het geval van analyses niet altijd mogelijk zijn omdat bijvoorbeeld bij bepaalde publieke personen altijd herleidbaar is om wie het gaat. Daarnaast geldt voor bepaalde coördinerende werkzaamheden dat het niet mogelijk is om deze te verrichten zonder dat er persoonsgegevens worden verstrekt aan de betrokken ketenpartners en kan dit ook niet op gepseudonimiseerde wijze. In het geval van bijvoorbeeld noodzakelijke coördinerende werkzaamheden rond een terugkerende Syriëganger die vervolgd dient te worden, kan het verstrekken van bijvoorbeeld de naam waarschijnlijk onvermijdelijk zijn. Een ander voorbeeld betreft een persoon waarvan het Nederlanderschap is ingetrokken die vrijkomt uit strafrechtelijke detentie en vreemdelingenbewaring niet (langer) mogelijk is.

Andere waarborgen die in de wet zijn opgenomen betreffen de opgenomen bewaartermijnen (artikel 3, vierde, vijfde en zesde lid), het feit dat online geen technische hulpmiddelen ingezet kunnen worden die op basis van profilering persoonsgegevens verzamelen, analyseren en combineren (artikel 3, tweede lid, van de wet) en de verplichting tot het verrichten van een gegevensbeschermingsaudit (artikel 5 van de wet). Zoals bij de inleiding weergegeven geeft de wet tevens de opdracht tot het stellen van regels bij algemene maatregel van bestuur die betrekking hebben op waarborgen. Het gaat om het stellen van technische, personele en organisatorische maatregelen en nadere regels over de gegevensbeschermingsaudit.

Vooraf verdient nog de vermelding dat, zoals ook bij de nota van wijziging bij - toen nog het wetsvoorstel - aan bod kwam, op grond van de definiëring in de AVG er al snel sprake is van persoonsgegevens. Niet alleen namen van personen zijn persoonsgegevens, maar bijvoorbeeld ook gegevens waardoor een persoon op indirecte wijze geïdentificeerd kan worden.[1] De waarborgen die zijn opgenomen zijn dan ook primair gericht op de bescherming van persoonsgegevens, met dien verstande dat deze onlosmakelijk verbonden zijn met gegevens die geen persoonsgegevens bevatten.

2.2. Werkwijze

[1] Kamerstukken II 2022/23, 35958, nr. 12, blz. 7-8.

Een eerste maatregel die met onderhavig besluit wordt genomen, heeft zowel als doel om de interne werkwijze aan te scherpen door de naleving van de bij en krachtens de wet gestelde regels te bevorderen, als de controleerbaarheid van de werkwijze te versterken door het registeren van een aantal gegevens.

Met artikel 2, eerste lid, van onderhavig besluit geldt dat de Minister het doel en de afbakening van werkzaamheden vastlegt die worden verricht ter uitvoering van artikel 2 van de wet. Met betrekking tot de vraag wat onder de afbakening van werkzaamheden moet worden verstaan geldt dat hier ruimte aan de praktijk wordt geboden om het abstractieniveau te bepalen, ook omdat maatwerk gewenst kan zijn. Het gaat erom dat er verantwoording kan worden afgelegd over de verrichte werkzaamheden, maar ook dat wordt stilgestaan bij de afbakening daarvan, zonder dat er op te groot detailniveau dient te worden vastgelegd waardoor de uitvoerbaarheid in het geding komt. Voor wat betreft de afbakening van werkzaamheden geldt in ieder geval dat indien toepassing wordt gegeven aan artikel 2, derde lid, van de wet, dit wordt vastgelegd. Op basis van dat artikel geldt namelijk dat het signaleren, analyseren en duiden van trends en fenomenen ten dienste van de coördinatietaak dient te staan, waarbij geldt dat de daarvoor benodigde informatie niet al op andere wijze beschikbaar is, zoals bij de totstandkoming van de wet aan bod kwam.[2]

Met artikel 2, tweede lid, van onderhavig besluit, geldt dat indien op grond van artikel 7 van de wet persoonsgegevens worden verstrekt, een aantal gegevens worden vastgelegd.

Ten eerste dient te worden vastgelegd of er sprake is van bijzondere of strafrechtelijke persoonsgegevens (artikel 2, eerste lid, onderdeel a). Bij de verwerking van dit type persoonsgegevens geldt immers op grond van de AVG een zwaarder regime.
Ten tweede geldt dat vastgelegd dient te worden op welke wijze artikel 7, tweede lid, van de wet is toegepast (artikel 2, eerste lid, onderdeel b). Artikel 7, tweede lid, van de wet regelt namelijk dat persoonsgegevens gepseudonimiseerd worden verstrekt, tenzij dit vanwege het doeleinde van de verwerking niet mogelijk is. Voor openbaarmaking van persoonsgegevens geldt de hoofdregel dat deze geanonimiseerd dienen te worden, tenzij dit vanwege het doeleinde van de verwerking niet mogelijk is. Op dit 'tenzij' is onder meer in de toelichting bij de nota van wijziging op de wet ingegaan.[3]

De wijze waarop aan deze verplichtingen invulling gegeven wordt zal in de werkprocessen worden vastgelegd op een wijze die uitvoerbaar is voor de praktijk. Daarbij kan er sprake zijn van maatwerk per type werkzaamheden. Zo is het bijvoorbeeld denkbaar dat er sprake is van een incidentele casus van een persoon van wie (mogelijk) een dreiging uitgaat en waarin coördinatie door de NCTV noodzakelijk is om het risico te mitigeren. Het kan dan nodig zijn dat de NCTV over de casus contact heeft met partners in het veiligheidsdomein om de samenwerking te bevorderen en dit niet goed mogelijk is zonder in dat contact steeds ook de persoonsgegevens van het individu te verstrekken. Het moet immers voor de gesprekspartners duidelijk zijn om welk individu het gaat. In deze gevallen wordt één keer de vastgelegd of voor deze casus bijzondere of strafrechtelijke gegevens verwerkt moeten worden en niet voorafgaand aan ieder afzonderlijk contact. Aangezien het communicatie in individuele casuïstiek betreft, kan in algemene zin worden gemotiveerd, dat het in die gevallen niet

[2] Kamerstukken II 2022/23, 35958, nr. 12, blz. 7.
[3] Kamerstukken II 2022/23, 35958, nr. 12, blz. 7.

mogelijk is gegevens gepseudonimiseerd te verstrekken. Partners zullen immers moeten weten om welke casus het gaat. Het zou het grote uitvoeringslasten met zich meebrengen als binnen hetzelfde dreigingsthema voor iedere afzonderlijk casus, of in het geval van een incidentele casus bij iedere tussenstap, dit steeds opnieuw zou moeten worden vastgelegd.

Tot slot geldt dat in artikel 2, tweede lid, onderdeel c, van onderhavig besluit wordt opgenomen dat indien een analyse nog persoonsgegevens bevat een motivering wordt vastgelegd waaruit blijkt dat is voldaan aan artikel 7, derde lid, van de wet. Artikel 7, derde lid, van de wet bepaalt immers dat er geen analyses kunnen worden verstrekt met de duiding van de uitingen van een persoon, waardoor die persoon in verband wordt gebracht met een trend of fenomeen. Als er dus analyses worden verstrekt aan organisaties waarin persoonsgegevens zijn opgenomen dient gemotiveerd te worden dat de desbetreffende persoon niet door die analyse in verband wordt gebracht met een trend of fenomeen en daardoor feitelijk aangemerkt wordt als gevaar of risico voor de nationale veiligheid. Een motivering kan in dit kader bijvoorbeeld zijn dat het gaat om een dader van een terroristische aanslag als Anders Breivik, een leider van een terroristische groepering, of een ander persoon die reeds op andere wijze onlosmakelijk verbonden is met een trend of fenomeen dan door het opnemen van persoonsgegevens in de analyse. Het opnemen van de motivering dient als aanvullende waarborg om te voorkomen dat personen waarvan nog niet op andere wijze is vastgesteld dat zij onderdeel zijn van een trend of fenomeen, niet door de verstrekking van een analyse gevolgen ondervinden. Het vastleggen van de motivering is zowel een interne waarborg om zorgvuldig om te gaan met de verstrekking van analyses waarin (herleidbare) persoonsgegevens staan opgenomen als een versterking van de mogelijkheid om de naleving van de wettelijke begrenzingen te controleren.

Voor de volledigheid dient er hier nog aan te worden herinnerd dat indien persoonsgegevens zijn geanonimiseerd dit geen persoonsgegevens meer zijn. In die gevallen is het vastleggen van de hierboven genoemde gegevens niet meer aan de orde.

2.3. Informatiebeveiligingsmaatregelen

Artikel 3 van onderhavig besluit bevat een set aan maatregelen die persoonsgegevens op meerdere manieren beschermen. Van belang is te benoemen dat de wet en onderhavig besluit primair aangrijpen op de bescherming van persoonsgegevens, maar informatiebeveiliging en de bescherming van persoonsgegevens geen gescheiden trajecten zijn, doordat persoonsgegevens en andere gegevens verweven zijn. Om die reden wordt hier gesproken over informatiebeveiliging waarmee ook de beveiliging van persoonsgegevens wordt bedoeld.

Op basis van artikel 3, eerste lid, onderdeel a, van onderhavig besluit, geldt dat de Minister in strategisch en tactisch risicogedreven informatiebeveiligingsbeleid voorziet, waarin is vastgelegd op welke wijze er toepassing wordt gegeven aan de daarvoor geldende normen, waaronder in ieder geval de door de Minister van Binnenlandse Zaken en Koninkrijksrelaties vastgestelde richtlijnen. Er is voor deze formulering gekozen om recht te doen aan het feit dat er verschillende normensets van belang zijn die zowel maatwerk vergen als aan verandering onderhevig zijn. Het doel van deze bepaling is dan ook dat het informatiebeveiligingsbeleid actueel wordt gehouden en controleerbaar is op welke wijze het wordt toegepast. Ook wordt daarmee recht gedaan aan het feit dat

informatiebeveiliging een cyclisch proces is van het vaststellen van maatregelen, interne controles, externe controles, gevolgd door verbetermaatregelen.

De normenkaders die relevant zijn voor de NCTV betreffen naast de AVG de Baseline Informatiebeveiliging Overheid (BIO), het Besluit Voorschrift Informatiebeveiliging Rijksoverheid 2007 (VIR) en het Besluit Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie 2013 (VIRBI) zoals vastgesteld door de Minister van Binnenlandse Zaken en Koninkrijksrelaties. Daarnaast wordt aangesloten bij de Algemene Beveiligingseisen Defensieopdrachten 2019 (ABDO 2019)[4] en het Volwassenheidsmodel Informatiebeveiliging van de Nederlandse Beroepsorganisatie van Accountants (NBA).[5] Deze normenkaders vergen maatwerk die in het beleid worden vastgelegd en geactualiseerd.

Met strategisch informatiebeveiligingsbeleid worden doelen vastgesteld die door middel van tactisch informatiebeveiligingsbeleid verder worden uitwerkt. Dit beleid is risicogedreven waardoor het passende beschermingsniveau en de bijbehorende maatregelen worden vastgesteld aan de hand van de risico's. Dit betekent ook dat indien de risico's veranderen het beleid daarin dient mee te meebewegen. Daarbij wordt cyclisch gewerkt doordat met het vaststellen van strategisch en tactisch risicogedreven informatiebeveiligingsbeleid, vervolgens concrete maatregelen worden geïmplementeerd. De werking en toepassing van deze maatregelen wordt periodiek intern door daartoe aangewezen functionarissen[6] gecontroleerd en geëvalueerd om de naleving van en kennis over de vastgestelde normen te beoordelen. Tot slot geldt dat door middels van onafhankelijke externe audits de effectiviteit van deze mechanismen en de naleving van de betreffende normen wordt gecontroleerd.

Een tweede maatregel is opgenomen in artikel 3, eerste lid, onderdeel b, waarin is opgenomen dat wordt voorzien in functiescheiding waardoor bij de toepassing van artikel 2 van de wet onderscheid wordt gemaakt tussen de rollen van opdrachtgever en opdrachtnemer. Concreet betekent dit bijvoorbeeld dat de persoon die vaststelt dat het signaleren, analyseren en duiden van een trend of fenomeen als bedoeld in artikel 2, derde lid, van de wet noodzakelijk is in verband met de coördinatietaak opgenomen in artikel 2, eerste en tweede lid, van de wet (opdrachtgever) niet tevens de persoon kan zijn die deze werkzaamheden verricht (opdrachtnemer). De wijze waarop invulling gegeven wordt aan de scheiding van deze rollen dient ingekleurd te worden en vastgelegd te worden in de werkprocessen. Daarbij kan onderscheid worden gemaakt tussen verschillende trajecten en type werkzaamheden. Het doel hiervan is om een intern toetsmechanisme dat extern controleerbaar is in te bouwen, waarbij steeds op het passende niveau en passend bij de situatie een beslissing wordt genomen over te verrichten werkzaamheden.

In lijn met het voorgaande wordt als derde maatregel in artikel 3, eerste lid, onderdeel c, het voorzien in een actuele autorisatiematrix vastgelegd. Een autorisatiematrix

[4] De ABDO ziet op beveiligingseisen die het Ministerie van Defensie hanteert bij het verlenen van opdrachten aan bedrijven.

[5] De NBA is een openbaar lichaam ingesteld op grond van artikel 2 van de Wet op het accountantsberoep.

[6] Interne functionarissen betreffen onder meer de functionaris voor gegevensbescherming ten aanzien van de naleving van de AVG, Chief Information Officer (CIO) en de Chief Information Security Officer (CISO).

betekent kort gezegd dat duidelijk is vastgelegd wie tot welke informatie toegang heeft en waarom. Dit zal worden ingericht op 'need to know' basis. Ook hier geldt dat de concrete invulling dient te worden vastgelegd.

Tot slot wordt als vierde maatregel in artikel 3, eerste lid, onderdeel d, een verplichting tot het loggen van zoekopdrachten die plaatsvinden in verband met het signaleren, analyseren en duiden van trends en fenomenen opgenomen. Op deze wijze is onder meer controleerbaar of er sprake is van 'onderzoek gericht op personen' (zoals opgenomen in artikel 2, derde lid, van de wet). Wellicht ten overvloede geldt dat in artikel 3, tweede lid, van onderhavig besluit is vastgelegd dat de gegevens die in verband met het loggen van zoekopdrachten worden vastgelegd, uitsluitend worden gebruikt voor controledoeleinden. Deze controles kunnen intern of extern van aard zijn, maar hebben als doel om de naleving van de bij of krachtens de wet gestelde normeringen te controleren en kunnen dus niet voor andere doeleinden worden ingezet.

2.4. Gegevensbeschermingsaudits

De wet verplicht in artikel 5, eerste lid, tot het zorgdragen voor het periodiek doen verrichten van gegevensbeschermingsaudits ten aanzien van het gebruik van publiek toegankelijke online bronnen. De reden is dat gegevens afkomstig van publiek toegankelijke online bronnen vaak betrekking zullen hebben op gegevens die persoonsgegevens bevatten en afkomstig zijn van sociale media. Dit rechtvaardigt wettelijk geregelde aanvullende bescherming. De wet bepaalt tevens dat indien uit de controleresultaten blijkt dat niet wordt voldaan aan de bij of krachtens de wet gestelde eisen, de Minister binnen een jaar een hercontrole laat uitvoeren op de onderdelen die niet voldeden aan de gestelde eisen.

Met onderhavig besluit wordt vastgelegd dat ieder jaar een interne gegevensbeschermingsaudit en iedere vier jaar een externe gegevensbeschermingsaudit wordt verricht. De eerste zes jaar na invoering van de wet geldt echter een hogere frequentie voor de externe audit, namelijk iedere twee jaar. De reden voor deze termijnen is dat de invoering van nieuwe regels een intensievere controle in de eerste periode vaak rechtvaardigen dan op langere termijn proportioneel is. Er is immers sprake van een nieuwe werkwijze en nieuwe systemen waar ervaring mee opgedaan moet worden.

Voor wat betreft de inhoud van de gegevensbeschermingsaudits geldt dat deze betrekking dienen te hebben op de wijze waarop is voorzien in maatregelen en procedures en de werking van deze maatregelen en procedures waarmee beoogd wordt in de borging van de wettelijke eisen te voorzien. Meer concreet: welke maatregelen worden genomen om ervoor te zorgen dat de wettelijke eisen worden nageleefd en werken deze. Zo niet, dan dient er een verbeterplan te worden opgesteld om bij te sturen.

3. Gevolgen en uitvoering

Onderhavig besluit brengt een aantal gevolgen met zich mee.

Allereerst betekent de vaststelling van onderhavig besluit dat de wet in werking kan treden en de coördinatietaak overeenkomstig de wet, met de daarbij behorende

begrenzingen en waarborgen, kan worden verricht. Dit betekent ook dat binnen de NCTV de werkprocessen overeenkomstig de wet en onderhavig besluit moeten zijn ingericht. Zoals bekend is voorafgaand aan de totstandkoming van de wet veel gebeurd, zijn werkzaamheden stilgelegd, keren werkzaamheden die in het verleden werden verricht niet terug onder de wet en geldt voor werkzaamheden die wel terugkeren dat deze op een andere manier worden verricht.

Met de invoering van de wet wordt de NCTV in staat gesteld om samen met partners de aanpak van dreigingen tegen de nationale veiligheid vorm te geven en de weerbaarheid te verhogen. Voor gemeenten betekent dit bijvoorbeeld dat zij weer goed geïnformeerd kunnen worden over (actuele) ontwikkelingen die voor de nationale veiligheid van belang zijn, zodat zij hun beleid daarop kunnen inrichten. Een belangrijk verschil met de situatie van vóór in werking treden van de wet en dit besluit is dat de NCTV de coördinatietaak en daarop gerichte analysewerkzaamheden alleen mag uitoefenen als dat de uitkomst is van een hierop toegesneden afwegings- en besluitvormingsproces. Zoals hiervoor al opgemerkt keren namelijk niet alle werkzaamheden terug waaraan de NCTV in het verleden uitvoering gaf. Ook dit zal voor samenwerkingspartners van de NCTV merkbaar zijn.

Conform de motie van de leden Mutluer (PvdA) en Sjoerdsma (D66)[7] zal binnen een jaar na inwerkingtreding van de wet een invoeringstoets worden uitgevoerd waarbij in ieder geval zal worden ingegaan op de vraag of de NCTV de coördinatietaak naar behoren kan uitvoeren zonder dat daarbij de grenzen van die taak overschreden worden. Met de uitvoering van de invoeringstoets wordt tevens de motie van het lid Michon-Derkzen (VVD)[8] meegenomen. In die laatste motie wordt de regering verzocht via de Vereniging Nederlandse Gemeenten (VNG) bij gemeenten te inventariseren wat hun ervaringen zijn met de NCTV, welke knelpunten zich in de praktijk voordoen bij de samenwerking met de NCTV en te bezien of de wet voldoende basis biedt om de knelpunten op te lossen.

Ter voorbereiding op de uitvoering van de wet zijn binnen de NCTV zowel de werkprocessen als het informatiebeveiligingsbeleid tegen het licht gehouden, de benodigde veranderingen in kaart gebracht, gevolgd door het opstarten van een traject om de veranderingen binnen de organisatie door te voeren. Daartoe zijn verschillende instrumenten ontwikkeld om te waarborgen dat de nieuwe werkwijze overeenkomstig de wettelijke eisen wordt verankerd binnen de organisatie. Ten aanzien van de werkwijze geldt dat er een gedegen afweging plaatsvindt, voorafgaand aan het uitvoeren van coördinerende werkzaamheden en het ten behoeve daarvan maken van analyses en het verwerken van persoonsgegevens. Daarnaast is er een compliance afdeling in oprichting, ten behoeve van de interne controle van het beleid en de uitvoering daarvan en worden de benodigde functionarissen en experts aangetrokken, waaronder de in artikel 4 van de wet bedoelde functionaris voor gegevensbescherming. Voor werkprocessen worden risico’s en passende maatregelen geïdentificeerd, toegepast, geëvalueerd en waar nodig bijgesteld. Voor medewerkers en nieuwe medewerkers is er een opleidingscurriculum in ontwikkeling, met als doel om de kennis en competenties van zowel nieuwe als huidige medewerkers voor zover nodig te verbeteren. Hierbij is ook extra aandacht voor culturele aspecten die van invloed zijn op de acceptatie en borging van nieuwe werkwijzen.

[7] Kamerstukken II, 2023/24, 35 958, nr. 18.
[8] Kamerstukken II, 2023/24, 35 958, nr. 19.

Voor burgers en bedrijven betekent de invoering van de wet en onderhavig besluit twee dingen. Ten eerste geldt dat het belang van de nationale veiligheid en het versterken van de weerbaarheid van de samenleving tegen dreigingen en risico's ook van belang is van burgers en bedrijven. Ten tweede geldt dat met de wet en de daarin aangebrachte begrenzingen en waarborgen ook de rechtszekerheid is gediend en de bescherming van persoonsgegevens is gewaarborgd.

Het besluit heeft geen gevolgen voor de regeldruk.

De financiële gevolgen van de invoering van de wet zijn bij de totstandkoming van de wet meegenomen. De financiële gevolgen zijn gering en worden opgevangen binnen het huidige budget van de NCTV.

Voor de Inspectie Justitie en Veiligheid (IJenV) brengt de invoering van de wet uitvoeringsgevolgen mee. De IJenV is bij gelegenheid van de consultatie gevraagd een uitvoeringstoets te verrichten. [Gereserveerd voor reactie uitvoeringstoets].

4. Consultatie

Onderhavig besluit is toegezonden aan de Autoriteit Persoonsgegevens (AP) voor advies, voorgelegd aan het Adviescollege Toetsing Regeldruk (ATR), gedurende vier weken geplaatst op internetconsultatie.

[Gereserveerd voor verwerking consultatie]

Artikelsgewijze toelichting

Artikel 1. Definitie
Dit artikel bevat de voor het besluit benodigde definitie.

Artikel 2. Werkwijze
Artikel 2, eerste lid, van onderhavig besluit, bepaalt dat het doel en de afbakening van de werkzaamheden die worden verricht ter uitvoering van artikel 2 van de wet worden vastgelegd. Hierop is in paragraaf 2.2. nader ingegaan.

Artikel 2, tweede lid, van onderhavig besluit, ziet op het vastleggen van een aantal gegevens indien op grond van artikel 7 van de wet persoonsgegevens worden verstrekt. In onderdeel a is geregeld dat wordt vastgelegd of er sprake is van bijzondere of strafrechtelijke persoonsgegevens. In onderdeel b is opgenomen dat wordt vastgelegd op welke wijze toepassing is gegeven aan artikel 7, tweede lid, van de wet. Tot slot bepaalt onderdeel c, dat indien de verstrekking ziet op een analyse als bedoeld in artikel 2, derde lid, van de wet, een motivering wordt vastgelegd dat is voldaan aan artikel 7, derde lid, van de wet. Op deze onderdelen is in paragraaf 2.2. nader ingegaan.

Artikel 3. Beschermingsmaatregelen
Artikel 3, eerste lid, onderdeel a, van onderhavig besluit bepaalt dat voor de verwerking van persoonsgegevens wordt voorzien in het vaststellen van een actueel, strategisch en tactisch risicogedreven informatiebeveiligingsbeleid, waarin is vastgelegd op welke wijze invulling wordt gegeven aan de daarvoor geldende normen, waaronder in ieder geval de meest recente door de Minister van Binnenlandse Zaken en Koninkrijksrelaties vastgestelde richtlijnen. In paragraaf 2.3 is toegelicht welke relevante normen momenteel toepasselijk zijn op het informatiebeveiligingsbeleid. Het BIO, VIR en VIRBI betreffen normen die zijn vastgesteld door de Minister van BZK. Daarnaast bevat de AVG uiteraard normen ten aanzien van de bescherming van persoonsgegevens.

Het verschil tussen strategisch en tactisch informatiebeveiligingsbeleid is de mate van gedetailleerdheid waarmee invulling wordt gegeven aan bovengenoemde normen. Strategisch beleid vormt de basis voor het tactische beleid door richting te geven aan de verdere invulling door middels van het tactische informatiebeveiligingsbeleid. Zo dient uit het strategische informatiebeveiligingsbeleid te volgen welke normen en bijbehorende beschermingsdoelen relevant zijn, welke nader worden uitgewerkt in tactisch beschermingsbeleid. Risicogedreven wil zeggen dat er per proces of systeem maatregelen worden getroffen die passend zijn. Dit betekent concreet dat indien een risico toeneemt, passende maatregelen getroffen dienen te worden die passend zijn voor het risiconiveau.

Artikel 3, eerste lid, onderdeel b, van onderhavig besluit ziet op het voorzien in functiescheiding waardoor de rollen van opdrachtgever en opdrachtnemer bij de uitvoering van artikel 2 van de wet gescheiden worden.

Artikel 3, eerste lid, onderdeel c, van onderhavig besluit ziet op het voorzien in een actuele autorisatiematrix. Met een autorisatiematrix wordt vastgelegd wie toegang heeft tot welke informatie om welke reden. Daarnaast dient deze actueel te zijn zodat indien

bijvoorbeeld een persoon belast met bepaalde taken andere werkzaamheden gaat verrichten, de autorisatie daarop wordt aangepast.

Artikel 3, eerste lid, onderdeel d, van onderhavig besluit bevat tot slot de verplichting tot het loggen van zoekopdrachten bij het raadplegen van publiek toegankelijke bronnen, als bedoeld in artikel 3, eerste lid, onderdeel a, van de wet, voor zover dit online bronnen zijn, ten behoeve van het signaleren, analyseren en duiden van trends en fenomenen als bedoeld in artikel 2, derde lid, van de wet. In artikel 3, tweede lid, van onderhavig besluit is vastgelegd dat de gegevens die in verband met het loggen van zoekopdrachten worden vastgelegd uitsluitend worden gebruikt voor controledoeleinden.

Artikel 4. Gegevensbeschermingsaudit
Artikel 4, eerste lid, van onderhavig besluit verplicht tot het jaarlijks verrichten van een interne gegevensbeschermingsaudit en iedere vier jaar tot het doen verrichten van een externe gegevensbeschermingsaudit ten aanzien van de in artikel 3, eerste lid, onderdeel a, van de wet bedoelde publiek toegankelijke bronnen, voor zover dit online bronnen zijn.

In artikel 4, tweede lid, is geregeld dat deze audits betrekking hebben op de wijze waarop is voorzien in maatregelen en procedures en de werking van deze maatregelen en procedures waarmee beoogd wordt in de borging van de wettelijke eisen te voorzien.

In artikel 4, derde lid, is vastgelegd dat gedurende de eerste zes jaar na inwerkingtreding van de wet minimale iedere twee jaar een externe gegevensbeschermingsaudit wordt verricht in plaats van iedere vier jaar.

Artikel 5. Wijziging Besluit politiegegevens

Artikel 5 wijzigt het Besluit politiegegevens met het oog op de invoering van de Wet coördinatie terrorismebestrijding en nationale veiligheid. Artikel 6 van die wet regelt de verstrekking van gegevens door overheidsorganisaties aan de Minister in verband met de uitvoering van de wet. Onderdeel f van artikel 6 van de wet regelt de verstrekking ten aanzien van andere taken en bevoegdheden dan de opgenomen organisaties, indien de betreffende wetgeving in de verstrekking voorziet met inachtneming van die wetgeving. Zoals toegelicht in de memorie van toelichting bij de wet ten aanzien van de verstrekking van politiegegevens geldt dat artikel 18 en 19 van de Wet politiegegevens het kader vormt voor de verstrekking van politiegegevens. Deze artikelen zijn uitgewerkt in het Besluit politiegegevens, waarvoor geldt dat in de artikelen in de artikelen 4:3, eerste lid, onderdeel a en artikel 4:6, eerste lid, de Wet coördinatie terrorismebestrijding en nationale veiligheid dient te worden toegevoegd. De wijziging in artikel 5 van onderhavig besluit regelt dit.

De noodzaak voor de verstrekking van deze gegevens is gelegen in het belang van de bescherming van de bescherming van de nationale veiligheid, die daarmee gediend is. De coördinatietaak van de NCTV heeft immers het verhogen van de weerbaarheid tegen dreigingen en risico's, het beschermen van de nationale veiligheidsbelangen en het voorkomen van maatschappelijke ontwrichting als doel.

De NCTV heeft politiegegevens nodig om uitvoering te kunnen geven aan deze coördinatietaak. Dit kan bijvoorbeeld gaan om analysewerkzaamheden die ten dienste van de coördinatietaak worden uitgevoerd. Gedacht kan worden aan een geweldsincident waaraan mogelijk een terroristisch motief ten grondslag ligt en waarbij de politie ten behoeve van de duiding door de NCTV (bijzondere) persoonsgegevens verstrekt aan de NCTV. De NCTV bepaalt op basis van deze duiding of en zo ja op welke wijze coördinatie noodzakelijk is. Ook kan de politie persoonsgegevens met de NCTV delen in het kader van casuscoördinatie. Hier kan gedacht worden aan het tegengaan van de dreiging van een individu door informatiedeling en samenwerking tussen partners te bevorderen. De politie deelt als partner in dat proces (persoons)gegevens met de NCTV.

Artikel 6. Inwerkingtreding
De inwerkingtreding van onderhavig besluit vindt bij koninklijk besluit plaats en zal tegelijkertijd plaatsvinden met de inwerkingtreding van de wet.

Artikel 7. Citeertitel
Dit artikel regelt de citeertitel van het besluit, namelijk Besluit coördinatie terrorismebestrijding en nationale veiligheid.