Ministerie van Justitie en Veiligheid

> Retouradres Postbus 20301 2500 EH Den Haag

Aan de Voorzitter van de Eerste Kamer
der Staten-Generaal
Postbus 20017
2500 EA DEN HAAG

Directie Wetgeving en Juridische Zaken
Staats-en Bestuursrecht

Turfmarkt 147
2511 DP Den Haag
Postbus 20301
2500 EH Den Haag
www.rijksoverheid.nl/jenv

Onze referentie
5978270

Bijlage(n)
1

Datum 11 december 2024
Betreft Voorhang ontwerp Besluit coördinatie terrorismebestrijding en nationale veiligheid

Hierbij bied ik u aan het ontwerpbesluit houdende regeling van technische, personele en organisatorische maatregelen en nadere regels omtrent gegevensbeschermingsaudits onder de Wet coördinatie terrorismebestrijding en nationale veiligheid (Besluit coördinatie terrorismebestrijding en nationale veiligheid). Voor de inhoud van het ontwerpbesluit verwijs ik naar de ontwerpnota van toelichting.

De voorlegging geschiedt in het kader van de wettelijk voorgeschreven voorhangprocedure opgenomen in artikel 10 van de Wet coördinatie terrorismebestrijding en nationale veiligheid en biedt uw Kamer de mogelijkheid zich uit te spreken over het ontwerpbesluit voordat het aan de Afdeling advisering van de Raad van State zal worden voorgelegd en vervolgens zal worden vastgesteld.

Op grond van de aangehaalde bepalingen geschiedt de voordracht aan de Koning ter verkrijging van het advies van de Afdeling advisering van de Raad van State over het ontwerpbesluit niet eerder dan vier weken nadat het ontwerpbesluit aan beide Kamers der Staten-Generaal is overgelegd.

Op grond van aanwijzing 2.38 van de Aanwijzingen voor de regelgeving wordt deze termijn in verband met het Kerstreces van uw Kamer verlengd tot 1 februari 2025.

Een gelijkluidende brief heb ik gezonden aan voorzitter van de Tweede Kamer der Staten-Generaal.

De Minister van Justitie en Veiligheid,

D.M. van Weel

WIJ WILLEM ALEXANDER,
BIJ DE GRATIE GODS,
KONING DER NEDERLANDEN,
PRINS VAN ORANJE-NASSAU,
ENZ. ENZ. ENZ.

Besluit van

houdende regeling van technische, personele en organisatorische maatregelen en nadere regels omtrent gegevensbeschermingsaudits ter uitvoering van de Wet coördinatie terrorismebestrijding en nationale veiligheid en tot wijziging van het Besluit politiegegevens (Besluit coördinatie terrorismebestrijding en nationale veiligheid)

Op de voordracht van Onze Minister van Justitie en Veiligheid van (datum voordracht), directie Wetgeving en Juridische Zaken, nr. (kenmerk voordracht);

Gelet op artikel 3, derde lid, en artikel 5, derde lid, van de Wet coördinatie terrorismebestrijding en nationale veiligheid en artikel 18, eerste lid, en artikel 23, tweede lid, van de Wet politiegegevens;

De Afdeling advisering van de Raad van State gehoord (advies van ..... (datum en nummer));

Gezien het nader rapport van Onze Minister van Justitie en Veiligheid (datum nader rapport), directie Wetgeving en Juridische Zaken, nr. (kenmerk nader rapport);

Hebben goedgevonden en verstaan:

Artikel 1. Definitie
In dit besluit wordt verstaan onder wet: Wet coördinatie terrorismebestrijding en nationale veiligheid.

Artikel 2. Werkwijze
1. Onze Minister legt het doel en de afbakening van de werkzaamheden vast die worden verricht ter uitvoering van artikel 2 van de wet.
2. Indien op grond van artikel 7, eerste lid, van de wet persoonsgegevens worden verstrekt legt Onze Minister vast:
   a. of er sprake is van bijzondere categorieën van persoonsgegevens of van persoonsgegevens van strafrechtelijke aard;
   b. op welke wijze artikel 7, tweede lid, van de wet is toegepast; en

c. indien de verstrekking betrekking heeft op een analyse van een trend of fenomeen als bedoeld in artikel 2, derde lid, van de wet: de motivering dat is voldaan aan artikel 7, derde lid, van de wet.

Artikel 3. Beschermingsmaatregelen

1. Onze Minister voorziet voor de verwerking van persoonsgegevens bij of krachtens de wet in:
   a. actueel strategisch en tactisch risicogebaseerd informatiebeveiligingsbeleid waarin is vastgelegd op welke wijze invulling wordt gegeven aan de daarvoor geldende normen, waaronder in ieder geval de meest recente door Onze Minister van Binnenlandse Zaken en Koninkrijksrelaties en Onze Minister-President, Minister van Algemene Zaken, vastgestelde richtlijnen;
   b. functiescheiding waardoor bij de uitvoering van de in artikel 2 van de wet bedoelde taak onderscheid wordt gemaakt in verschillende taken en rollen;
   c. maatregelen waarmee de toegang tot gegevens op zorgvuldige wijze wordt geregeld;
   d. het loggen van zoekopdrachten van de in artikel 3, eerste lid, onderdeel a, van de wet bedoelde publiek toegankelijke bronnen, voor zover dit onlinebronnen zijn en deze bronnen kunnen worden aangemerkt als sociale media, ten behoeve van het signaleren, analyseren en duiden van trends en fenomenen als bedoeld in artikel 2, derde lid, van de wet.
2. De gegevens die in verband met het loggen als bedoeld in het eerste lid, onderdeel d, worden vastgelegd, worden uitsluitend gebruikt voor controledoeleinden. Deze gegevens worden ten minste tot de datum waarop de laatste externe gegevensbeschermingsaudit, bedoeld in artikel 4, eerste lid, heeft plaatsgevonden bewaard.

Artikel 4. Gegevensbeschermingsaudit

1. Onze Minister laat iedere vier jaar door middel van een externe gegevensbeschermingsaudit de wijze waarop uitvoering wordt gegeven aan de bij en krachtens de wet gestelde regels ten aanzien de in artikel 3, eerste lid, onderdeel a, van de wet bedoelde publiek toegankelijke bronnen, voor zover dit onlinebronnen zijn, in verband met het signaleren, analyseren en duiden van trends en fenomenen, controleren.
2. De in het eerste lid bedoelde controles hebben betrekking 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.
3. In afwijking van het eerste lid laat Onze Minister de eerste zes jaar na inwerkingtreding van de wet eens in de twee jaar een externe gegevensbeschermingsaudit verrichten.
4. Onze Minister stuurt een afschrift van de controleresultaten van de externe gegevensbeschermingsaudit, bedoeld in het eerste lid, aan de Autoriteit Persoonsgegevens.
5. Ter voorbereiding op de controles, bedoeld in het eerste lid, laat Onze Minister ieder jaar een interne gegevensbeschermingsaudit verrichten.

Artikel 5. Wijziging Besluit politiegegevens[1]

Het Besluit politiegegevens wordt als volgt gewijzigd:

A

Aan artikel 4:3, eerste lid, onderdeel a, wordt onder vervanging van de punt door een puntkomma aan het slot van dat lid, een onderdeel waarvan de nummering aansluit op het laatste onderdeel toegevoegd, luidende:
#°. de uitvoering van artikel 2 van de Wet coördinatie terrorismebestrijding en nationale veiligheid.

B

Aan artikel 4:6, eerste lid, wordt onder vervanging van de punt door een puntkomma aan het slot van dat lid, een onderdeel waarvan de letteraanduiding alfabetisch aansluit op het laatste onderdeel toegevoegd, luidende:
#. de ambtenaren van Onze Minister van Justitie en Veiligheid ten behoeve van de taak in artikel 2 van de Wet coördinatie terrorismebestrijding en nationale veiligheid.

Artikel 6. Inwerkingtreding
Dit besluit treedt in werking op een koninklijk besluit te bepalen tijdstip.

Artikel 7. Citeertitel
Dit besluit wordt aangehaald als: Besluit coördinatie terrorismebestrijding en nationale veiligheid.

Lasten en bevelen dat dit besluit met de daarbij behorende nota van toelichting in het Staatsblad zal worden geplaatst.

De Minister van Justitie en Veiligheid,

[1] *Vanwege meerdere amvb's die in procedure zijn tot wijziging van het Besluit politiegegevens, zal de nummering later in de procedure worden aangepast aan de meest recente stand van zaken.*

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 die dienen ter bescherming van persoonsgegevens. 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 onlinebronnen 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 aanleiding van de wet werd gevormd door de constatering dat voor de verwerking van persoonsgegevens die vereist is voor de uitvoering van een aantal werkzaamheden van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (hierna: NCTV) een wettelijke grondslag vereist is.[2] De wet voorziet in deze grondslag in de vorm van de wettelijke taak, bedoeld in artikel 6, eerste lid, onderdeel e, en lidstatelijk recht als bedoeld in artikel 9, eerste lid, onderdeel g, van de Algemene Verordening Gegevensbescherming (hierna: AVG). Daarnaast bevat de wet diverse begrenzingen en waarborgen vanwege deze verwerking van persoonsgegevens. Deze hebben zowel als doel om persoonsgegevens te beschermen, als de naleving van de AVG te versterken en deze naleving controleerbaar te maken.

Zoals ook in de wetgeschiedenis aan bod kwam is in dit kader van belang om te benadrukken dat er al snel sprake is van een verwerking van persoonsgegevens in de zin van de AVG door de brede definiëring van «verwerking» in die verordening. Dus ook al is het doel niet om persoonsgegevens te verwerken, het feit dat in gegevens ook persoonsgegevens voorkomen en deze gegevens worden verwerkt, maakt dat er sprake is van de verwerking van persoonsgegevens waarvoor de regels van de AVG gelden.[3]

---

[2] Zie onder meer de brief van de Minister van Justitie en Veiligheid van 12 april 2021 (Kamerstukken II 2020/21, 32761, nr. 180)

[3] Zie onder meer de nota naar aanleiding van het verslag (Kamerstukken II 2023/24, 35958, nr. 11, p. 7)

Daarbij gaat het niet alleen om gegevens waardoor een persoon meteen kan worden geïdentificeerd, maar ook om gegevens waardoor een persoon indirect identificeerbaar is door een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.

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 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). Daarbij zijn steeds diverse begrenzingen en waarborgen opgenomen.

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, maar wel maatregelen nodig zijn.

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. Deze regels vormen feitelijk een nadere concretisering van de verplichting tot het stellen van waarborgen waar de AVG om vraagt, waarbij is voorzien in waarborgen die passend zijn voor de verwerking en situatie die het betreft.

Daarbij is gekeken naar de versterking van de controleerbaarheid van de naleving waarbij er controle zal 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.

In onderhavige amvb zijn aanvullende waarborgen en de nadere uitwerking van wettelijke waarborgen opgenomen.

2.2. Werkwijze

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.[4]

[4] *Kamerstukken II 2022/23, 35958, nr. 12, p. 7.*

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 wordt vastgelegd.

Ten eerste dient te worden vastgelegd of er sprake is van bijzondere categorieën van persoonsgegevens of van persoonsgegevens van strafrechtelijke aard (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.[5]
Tot slot geldt 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 2, tweede lid, onderdeel c). 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. Beschermingsmaatregelen

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.

[5] *Kamerstukken II 2022/23, 35958, nr. 12, p. 7.*

Op basis van artikel 3, eerste lid, onderdeel a, van onderhavig besluit, geldt dat de Minister in strategisch en tactisch risicogebaseerd 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 en door de Minister-President, Minister van Algemene Zaken vastgestelde richtlijnen (zie hierna). 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) zoals vastgesteld door de Minister van Binnenlandse Zaken en Koninkrijksrelaties, het Besluit Voorschrift Informatiebeveiliging Rijksoverheid 2007 (VIR) en het Besluit Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie 2013 (VIRBI) zoals vastgesteld door de Minister-President, Minister van Algemene Zaken. 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 uitgewerkt. Dit beleid is risicogebaseerd 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 of de maatregelen daarin dient mee te meebewegen. Daarbij wordt cyclisch gewerkt doordat met het vaststellen van strategisch en tactisch risicogebaseerd 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 middel 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 bij de uitvoering van de in artikel 2 van de wet opgenomen taak wordt voorzien in onderscheid tussen verschillende taken en rollen (functiescheiding). Concreet betekent dit bijvoorbeeld dat het vaststellen van de noodzaak tot het signaleren, analyseren en duiden van een trend of fenomeen als bedoeld in artikel 2, derde lid, van de wet in verband met de coördinatietaak opgenomen in artikel 2, eerste en tweede lid, van de wet (rol opdrachtgever) niet kan samengaan met de uitvoering van deze werkzaamheden (rol 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.

---

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

In lijn met het voorgaande wordt als derde maatregel in artikel 3, eerste lid, onderdeel c, voorgesteld het voorzien in maatregelen waarmee de toegang tot gegevens op zorgvuldige wijze wordt geregeld. Dit betekent kort gezegd dat duidelijk is vastgelegd welke gebruikersrollen en -groepen tot welke gegevens(bronnen), applicaties, functionaliteiten en systemen toegang hebben, welke acties (zoals lezen, schrijven, wijzigen, verwijderen) zij kunnen uitvoeren 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 vastgelegd tot het loggen van zoekopdrachten van publiek toegankelijke bronnen, als bedoeld in artikel 3, eerste lid, onderdeel a, van de wet, indien dit onlinebronnen zijn en voor zover dit sociale media betreft, ten behoeve van het signaleren, analyseren en duiden van trends en fenomenen als bedoeld in artikel 2, derde lid, van de wet. Publiek toegankelijke online bronnen (zoals omschreven in de memorie van toelichting bij de wet)[7] omvatten meerdere gegevensbronnen omdat ook openbare nieuwssites als publiek toegankelijke online bron kunnen worden beschouwd.

Uit de systematiek van de AVG volgt dat er met de verwerking van persoonsgegevens dient te worden gekeken naar risico's voor betrokkenen en passende beschermingsmaatregelen dienen te worden getroffen. De grootste risico's liggen bij het raadplegen van sociale media zoals Twitter (thans 'X') zodat daar de zwaarste waarborg voor wordt opgenomen. Er zijn verschillende afbakeningsroutes te volgen, bijvoorbeeld de inhoud van de berichtgeving ('content') of de bron van berichtgeving. Zo kan een krantenartikel geplaatst worden op sociale media, maar het plaatsen van een krantenartikel zal niet snel worden aangemerkt als 'sociale media content'.[8] Er is echter voor gekozen om geen onderscheid te maken naar type inhoud, maar naar type bron omdat daarmee het belang van de bescherming van de persoonlijke levenssfeer van betrokkenen het meest gediend is. Concreet betekent dit dat zal worden voorzien in loggen van zoekopdrachten van sociale media voor analysedoeleinden.[9] Met het oog op uitvoerbaarheid en beheersbaarheid kunnen er bij andersoortige raadplegingen van publiek toegankelijke onlinebronnen zoals bijvoorbeeld nieuwsberichten of wetenschappelijke publicaties, lichtere maatregelen worden genomen, zoals bronvermelding bij analyseproducten.

Het doel van het loggen van zoekopdrachten van sociale media voor analysedoeleinden is om het doel waarvoor deze bronnen zijn gebruikt vast te kunnen stellen. De logbestanden zullen dan ook die gegevens moeten bevatten waarmee dit vastgesteld kan worden. Er wordt ruimte gelaten aan de toepassing in de praktijk om dit op een dusdanige manier in te richten dat hieraan wordt voldaan en de controle zo optimaal

---

[7] Kamerstukken II 2022/23, 35958, nr. 3, p. 14-16.

[8] Criteria die nog als actueel kunnen worden beschouwd over wanneer sprake is van content op sociale media zijn te vinden in "Kaplan, Andreas & Haenlein, Michael (2010), Users of the World, Unite! The Challenges and Opportunities of Social Media, Business Horizons Volume 53,Issue 1, 59-68".

[9] Het Rijksprogramma voor Duurzaam Digitale Informatiehuishoudingbestaan hanteert thans als uitleg van het begrip sociale media "een grote diversiteit aan online platformen waarin gebruikers met elkaar in contact komen door het plaatsen en delen van inhoud (content) of het reageren hierop.

mogelijk kan plaatsvinden. Daarbij geldt dat bij het loggen van zoekopdrachten ook relevante contextinformatie wordt vastgelegd, zoals de relatie met de coördinatietaak, de verrichte analyse en het doel van de zoekopdracht en vanuit welke rol deze is uitgevoerd. Ook valt te denken aan nadere herleidbaarheid naar een onderzoek, betrokken medewerkers en data en tijden. Deze maatregel maakt controleerbaar of er met het signaleren, analyseren en duiden van trends en fenomenen geen 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. Tot slot is vastgelegd dat de logbestanden tenminste tot de datum waarop de laatste externe gegevensbeschermingsaudit heeft plaatsgevonden worden bewaard.

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 onlinebronnen. De reden is dat gegevens afkomstig van publiek toegankelijke onlinebronnen vaak persoonsgegevens bevatten en afkomstig kunnen 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 in artikel 4, eerste lid, vastgelegd dat iedere vier jaar een externe gegevensbeschermingsaudit wordt verricht. De eerste zes jaar na invoering van de wet geldt echter een hogere frequentie voor deze audit, namelijk iedere twee jaar. De reden voor deze termijnen is dat de invoering van nieuwe regels een intensievere controle in de eerste periode rechtvaardigen dan op langere termijn proportioneel is. Er is immers sprake van een nieuwe werkwijze en nieuwe systemen waar ervaring op gedaan mee moet worden. Dezelfde intensiviteit op langere termijn is echter niet proportioneel.

Voor wat betreft de inhoud van de gegevensbeschermingsaudits geldt op grond van artikel 4, tweede lid, 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 en geldt de bovengenoemde verplichting tot hercontrole. Een afschrift van de controleresultaten van de gegevensbeschermingsaudit wordt op grond van artikel 4, derde lid, van onderhavig besluit aan de Autoriteit Persoonsgegevens gezonden.

Tot slot geldt dat op grond van het voorgestelde artikel 4, vijfde lid, er jaarlijks een interne gegevensbeschermingsaudit wordt verricht ter voorbereiding op de externe controles.

2.5. Overige wijzigingen

Tot slot geldt dat, zoals aan bod kwam in de toelichting bij artikel 6 van de wet waarin de verstrekking van gegevens door organisaties aan de Minister is geregeld, er een aantal algemene wetten zijn met een specifiek verstrekkingenregime. Deze vallen onder artikel 6, onderdeel f van de wet. Voor de verstrekking van politiegegevens geldt dat deze verstrekking niet op wetsniveau is geregeld maar op amvb-niveau in het Besluit politiegegevens. Deze wijziging wordt dan ook met onderhavige amvb geregeld en wordt nader toegelicht in het artikelsgewijze deel van deze toelichting bij artikel 5.

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 ook 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)[10] 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)[11] 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.

[10] *Kamerstukken II 2023/24, 35 958, nr. 18.*
[11] *Kamerstukken II 2023/24, 35 958, nr. 19.*

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. Bij het opstellen van de amvb is ook steeds gekeken naar de juiste balans tussen goede waarborgen en uitvoerbaarheid. De verwachting is dat de ontwikkelde normen uitvoerbaar zijn.

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 voor 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. De IJenV heeft op 3 juni jl. een uitvoerings- en handhavingstoets uitgebracht met opmerkingen, aandachtspunten en verbetersuggesties. Deze hebben onder meer geleid tot aanvulling en verduidelijk van de toelichting en komen hierna aan bod.

Middels de bovengenoemde motie van de leden Mutluer en Sjoerdsma van 23 oktober 2023[12] is de regering verzocht één jaar na inwerkingtreding van de wet een invoeringstoets uit te voeren die ten minste ingaat op de vraag of de NCTV de coördinatietaak naar behoren kan uitvoeren zonder dat daarbij de grenzen van die taak overschreden worden. De IJenV geeft aan het tevens als taak te zien om input te geven voor deze toets. Hieraan zal gehoor worden gegeven.

[12] *Kamerstukken II 2023/24, 35958, nr. 18.*

Voor wat betreft de bepaling opgenomen in artikel 3, eerste lid, van het ontwerpbesluit geeft de IJenV ten aanzien van de informatiebeveiligingsbeleid aan dat het wenselijk is dit breder te trekken dan de bescherming van de persoonsgegevens. Van belang is in dit kader dat artikel 3 een uitvloeisel is van verplichtingen die de AVG meebrengt. Zoals in de memorie van toelichting uiteengezet, vereist de AVG dat bij de verwerking van persoonsgegevens de risico's voor betrokkenen in kaart worden gebracht en de beoogde maatregelen om die risico's aan te pakken. Dit heeft ertoe geleid dat er een grondslag is gecreëerd om – naast de waarborgen die in de wet zijn opgenomen – bij algemene maatregel van bestuur regels te stellen met betrekking tot te nemen technische, personele en organisatorische maatregelen, waaronder regels over functiescheiding, autorisatie voor het gebruik van bepaalde systemen, opslag en beveiliging. Deze regels waren in het oorspronkelijke wetsvoorstel in de toelichting als voorbeeld genoemd maar zijn in navolging van het advies van de AP bij de wet opgenomen in de grondslag.
Het voorgaande neemt overigens niet weg dat er wel degelijk een breder beveiligingsbeleid wordt gevoerd. Dit vloeit echter niet voort uit de Wet.
In reactie op de opmerkingen van de IJenV op dit terrein geldt dat voor wat betreft het voorzien in actueel strategisch en tactisch risicogebaseerd informatiebeveiligingsbeleid, uiteraard ook volgt dat dit beleid ook daadwerkelijk dient te worden uitgevoerd. Ook geldt dat dit beleid tevens waarborgen ten aanzien van de opslag van gegevens omvat.

De opmerkingen van de IJenV over het inregelen van autorisaties op rollen en over loggen zijn overgenomen en hebben geleid tot een aanscherping van de formulering in de artikelen en een uitbreiding van de toelichting.

Voor wat betreft de uitvoering van de gegevensbeschermingsaudits geldt in reactie op de vragen van de IJenV hierover dat het van belang is te benadrukkend dat deze audits niet uitgevoerd worden door de functionaris voor gegevensbescherming (f-g). Dit zou schuren met de onafhankelijke rol die de f-g vervult, waarbij geldt dat de taken die de f-g vervult rechtstreeks volgen uit de AVG.

Voor wat betreft de opmerkingen over de taakuitvoering van de IJenV het volgende.
Op grond van artikel 5a van de wet is expliciet gemaakt dat de Minister van Justitie en Veiligheid de wijze waarop uitvoering wordt gegeven aan de in artikel 2 van de wet bedoelde taak laat toetsen en dat een rapportage van de resultaten van deze toetsing aan de Staten-Generaal wordt gezonden. Naar aanleiding van de vragen hierover van de IJenV geldt dat hiermee inderdaad is beoogd aan te sluiten bij het Protocol voor de werkwijze van de IJenV en het relatiestatuut.

Verder geldt dat het uiteraard van belang is dat de IJenV toegang krijgt tot de gegevens die nodig zijn om haar taak te kunnen uitvoeren. Deze toegang wordt uiteraard verleend. Een vergelijking met de wettelijke regeling voor toezicht zoals opgenomen in de Wet op de inlichtingen- en veiligheidsdiensten 2017 ligt echter niet voor de hand gelet op de verschillende wijze waarop de CTIVD en de IJenV als Rijksinspectie zijn ingebed in het recht, naast het feit dat de werkzaamheden van de AIVD en de MIVD onder de Wiv 2017 wezenlijk verschillen van de werkzaamheden van andere organisaties die het belang van de nationale veiligheid dienen, waaronder de NCTV. Daarnaast geldt dat de vraag naar de wijze waarop de positie van IJenV is geregeld breder is dan onderhavig besluit of de wet waarop deze is gebaseerd en in dit bredere kader betrokken dient te worden.

Tot slot geldt naar aanleiding van de vraag van de IJenV dat de verwerking van persoonsgegevens door de IJenV een met de oorspronkelijke verwerking verenigbaar doel is nu deze betrekking heeft op de controle op de werkzaamheden van de NCTV en er geen sprake is van een verzelfstandige organisatie met eigen rechtspersoonlijkheid. De IJenV benadrukt verder het feit dat de IJenV en de AP ieder als toezichthouder hun eigen taakstelling hebben en dat deze taakstellingen in elkaars verlengde liggen. Beide zijn complementair aan elkaar waarbij het uitgangspunt moet zijn dat sprake gaat zijn van integraal en effectief toezicht. De IJenV geeft aan dat het van belang is dat een onevenredige toezicht last op de NCTV wordt voorkomen. Dit onderstreept het belang dat de IJenV en de AP onderling goede afspraken maken.

In de aanloop naar de invoering van de wet zal tussen de IJenV en de NCTV nader gesproken worden over de eventuele nog resterende praktische punten waar de IJenV in haar advies naar verwijst.

4. Consultatie

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

Via internetconsultatie zijn geen reacties ontvangen.

ATR heeft het dossier niet geselecteerd voor een formeel advies, omdat het geen gevolgen voor de regeldruk heeft.

De AP heeft op 3 oktober jl. een wetgevingstoets uitgebracht waarin de AP concludeert dat uit het oogpunt van effectief toezicht wenselijk is dat de resultaten van de uit te voeren gegevensbeschermingsaudits actief aan de AP worden gezonden, zodat aanpassing van het conceptbesluit aangewezen is. Deze aanpassing heeft plaatsgevonden door deze toezending vast te leggen in het vierde lid van artikel 4.

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 persoonsgegevens of gegevens van strafrechtelijke aard. 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 risicogebaseerd informatiebeveiligingsbeleid, waarin is vastgelegd op welke wijze invulling wordt gegeven aan de daarvoor geldende normen. In paragraaf 2.3 is toegelicht welke relevante normen momenteel toepasselijk zijn op het informatiebeveiligingsbeleid. De BIO, het VIR en het VIRBI betreffen normen die zijn vastgesteld door respectievelijk de Minister van BZK en de Minister-President, Minister van Algemene Zaken. 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. Risicogebaseerd 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 bij de uitvoering van de wet onderscheid wordt gemaakt in verschillende taken en rollen. Dit is in paragraaf 2.3 nader toegelicht.

Artikel 3, eerste lid, onderdeel c, van onderhavig besluit verplicht tot het voorzien in maatregelen waarmee de toegang tot gegevens op zorgvuldige wijze wordt geregeld. Ook dit onderdeel is nader toegelicht in paragraaf 2.3.

Artikel 3, eerste lid, onderdeel d, van onderhavig besluit bevat een verplichting tot het loggen van zoekopdrachten in publiek toegankelijke bronnen, als bedoeld in artikel 3, eerste lid, onderdeel a, van de wet, voor zover dit online bronnen zijn en deze bronnen als sociale media kunnen worden aangemerkt, 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 loggegevens die worden vastgelegd uitsluitend worden gebruikt voor controledoeleinden. Daarnaast dienen deze gegevens tenminste tot de laatste externe gegevensbeschermingsaudit als bedoeld in artikel 4, eerste lid, heeft plaatsgevonden te worden bewaard.

Artikel 4. Gegevensbeschermingsaudit
Artikel 4, eerste lid, van onderhavig besluit verplicht om iedere vier jaar middels een externe gegevensbeschermingsaudit de wijze waarop uitvoering wordt gegeven aan de bij of krachtens de wet gestelde regels ten aanzien van de in artikel 3, tweede lid, onderdeel a, van de wet bedoelde publiek toegankelijke bronnen, voor zover dit online bronnen zijn, in verband met het signaleren, analyseren en duiden van trends en fenomenen te laten controleren. In artikel 4, derde lid, is vastgelegd dat gedurende de eerste zes jaar na inwerkingtreding van de wet minimaal iedere twee jaar een externe gegevensbeschermingsaudit wordt verricht in plaats van iedere vier jaar.

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.

Op grond van artikel 4, vierde lid, wordt een afschrift van de controleresultaten van de externe gegevensbeschermingsaudit als bedoeld in het eerste lid aan de Autoriteit Persoonsgegevens gestuurd.

Tot slot is in artikel 4, vijfde lid opgenomen dat er jaarlijks een interne gegevensbeschermingsaudit zal worden uitgevoerd ter voorbereiding van de externe gegevensbeschermingsaudit als bedoeld in het eerste lid.

Het voorgaande is nader toegelicht in paragraaf 2.4.

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.

De Minister van Justitie en Veiligheid,